



## **Cisco IOS Carrier Ethernet Command Reference**

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### ais through ethernet cfm logging 1

ais 3

action switch ring g8032 clear instance 5

action switch ring g8032 instance 7

alarm 9

announce interval 11

announce timeout 13

aps-channel 14

backbone interface 15

bridge-domain (global) 16

bridge-domain (service instance) 18

bridge-domain from-encapsulation 21

cfm encapsulation 23

cfm mep domain 25

channel-group (interface) 28

clear bridge-domain mac-table 34

clear ethernet cfm ais 36

clear ethernet cfm errors 39

clear ethernet cfm maintenance-points remote 42

clear ethernet cfm statistics 44

clear ethernet cfm traceroute-cache 45

clear ethernet event microwave data 46

clear ethernet event microwave statistics 47

clear ethernet lmi statistics 48

clear ethernet oam statistics 50

clear ethernet ring g8032 statistics 52

clear ethernet service instance 53

clear lldp 55

clock destination	57
clock-port	58
clock source (PTP)	60
continuity-check	61
cos (CFM)	63
delay-req interval	64
description (Ethernet ring)	66
description (mac-tunnel)	67
disable (CFM-AIS-link)	68
encapsulation dot1ah isid	69
errdisable recovery cause mac-security	70
errdisable recovery cause mlacp-minlink	72
ethernet cfm ais	73
ethernet cfm ais link-status	75
ethernet cfm ais link-status global	77
ethernet cfm alarm	78
ethernet cfm cc	80
ethernet cfm cc enable level evc	84
ethernet cfm cc enable level vlan	86
ethernet cfm distribution enable	89
ethernet cfm domain level	90
ethernet cfm enable (interface)	92
ethernet cfm enable	93
ethernet cfm global	94
ethernet cfm ieee	95
ethernet cfm interface	96
ethernet cfm logging	97
<hr/>	
<b>CHAPTER 2</b>	<b>ethernet cfm mep crosscheck through location prefer</b> 99
	ethernet cfm mep crosscheck 102
	ethernet cfm mep crosscheck start-delay 105
	ethernet cfm mep domain mpid 107
	ethernet cfm mep level mpid vlan 109
	ethernet cfm mip 113
	ethernet cfm mip level 115

ethernet cfm slm max	117
ethernet cfm slm timeout	119
ethernet cfm traceroute cache	121
ethernet cfm traceroute cache hold-time	123
ethernet cfm traceroute cache size	125
ethernet event microwave	127
ethernet evc	129
ethernet lmi	131
ethernet lmi ce-vlan map	133
ethernet lmi global	135
ethernet lmi interface	137
ethernet loopback local interface	139
ethernet loopback permit	141
ethernet mac-flush notification mirp	143
ethernet mac limit action flooding disable	145
ethernet mac limit maximum addresses	147
ethernet mac-tunnel virtual	148
ethernet oam	149
ethernet oam link-monitor frame	152
ethernet oam link-monitor frame-period	154
ethernet oam link-monitor frame-seconds	156
ethernet oam link-monitor high-threshold action	158
ethernet oam link-monitor on	160
ethernet oam link-monitor receive-crc	162
ethernet oam link-monitor supported	164
ethernet oam link-monitor symbol-period	166
ethernet oam link-monitor transmit-crc	168
ethernet oam mib log size	170
ethernet oam remote-loopback	171
ethernet oam remote-loopback (interface)	173
ethernet ring g8032	175
ethernet ring g8032 profile	176
ethernet subscriber	177
ethernet subscriber session	179
ethernet subscriber static	181

ethernet tcn-propagation 183  
ethernet uni 184  
event ethernet microwave clear-sd 186  
event ethernet microwave sd 188  
exclusion-list 190  
id (CFM) 192  
inclusion-list 193  
initiator unclassified vlan 195  
input 197  
instance (Ethernet ring) 199  
l2 subscriber 200  
lacp active-port distribution automatic 202  
lacp direct-loadswap 204  
lacp failover 205  
lacp fast-switchover 207  
lacp max-bundle 209  
lacp min-bundle 211  
lacp port-priority 213  
lacp rate 215  
lacp system-priority 217  
level (CFM-AIS-link) 219  
level 220  
lldp 221  
lldp (interface) 224  
location 226  
location (interface) 227  
location civic-location identifier 229  
location civic-location-id 232  
location custom-location identifier 235  
location custom-location-id 237  
location geo-location identifier 239  
location geo-location-id 241  
location prefer 243

mac access-group in 248

mac aging-time 250

mac limit action flooding disable 251

mac limit maximum addresses 253

mac limit maximum addresses (service instance) 254

mac security 255

mac static address 259

mac tunnel address destination default 261

mac tunnel address destination map 262

maximum meps 263

mep archive-hold-time 264

mep crosscheck mpid evc 266

mep crosscheck mpid vlan 268

mep mpid 270

mip auto-create 271

mip auto-create (cfm-srv) 272

mlacp interchassis group 273

mlacp lag-priority 274

mlacp node-id 276

mlacp system-mac 278

mlacp system-priority 280

monitor loss counter 282

monitor service instance 283

non-revertive 284

oam protocol 285

open-ring 287

output 288

peer 290

period (CFM-AIS-link) 292

ping ethernet 293

ping ethernet evc 300

ping ethernet mpid vlan 302

ping ethernet vlan 304

port0 306

port0 service instance 307

port1	308
port1 service instance	309
port-channel load-balance	310
port-channel load-balance (interface)	313
port-channel load-balance mpls	315
port-channel load-balance weighted rebalance	317
priority1	319
priority2	320
profile	321
pseudowire (Layer 2)	322
ptp clock	324
rewrite egress tag	326
rewrite ingress tag	328
rpl	331
sender-id	332
sender-id (CFM-srv)	333
service (CFM-srv)	334
service evc	336
service icc	339
service instance dynamic	341
service instance ethernet	343
service instance ethernet (mac-tunnel)	346
service vlan	347
service-policy type control policy	349
show bridge-domain	351
show cfmpal	355
show ethernet cfm domain	357
show ethernet cfm errors	360
<b>show ethernet cfm maintenance-points local through weight</b>	<b>367</b>
show ethernet cfm maintenance-points local	370
show ethernet cfm maintenance-points remote	376
show ethernet cfm maintenance-points remote crosscheck	381
show ethernet cfm maintenance-points remote detail	385
show ethernet cfm mpdb	389

---

**CHAPTER 4**



[show ethernet cfm pm](#) 393

[show ethernet cfm smep](#) 395

[show ethernet cfm statistics](#) 397

[show ethernet cfm traceroute-cache](#) 400

[show ethernet event microwave statistics](#) 403

[show ethernet event microwave status](#) 404

[show ethernet lmi](#) 406

[show ethernet loopback](#) 413

[show ethernet mac-tunnel engine slot](#) 415

[show ethernet oam debug link-monitor](#) 416

[show ethernet oam discovery](#) 418

[show ethernet oam runtime](#) 421

[show ethernet oam statistics](#) 424

[show ethernet oam status](#) 427

[show ethernet oam summary](#) 431

[show ethernet ring g8032 brief](#) 433

[show ethernet ring g8032 configuration](#) 435

[show ethernet ring g8032 port status](#) 437

[show ethernet ring g8032 profile](#) 438

[show ethernet ring g8032 statistics](#) 439

[show ethernet ring g8032 status](#) 441

[show ethernet ring g8032 summary](#) 444

[show ethernet ring g8032 trace](#) 446

[show ethernet service dynamic](#) 447

[show ethernet service evc](#) 450

[show ethernet service instance](#) 452

[show ethernet service interface](#) 458

[show ethernet service mac-tunnel](#) 461

[show lacp](#) 464

[show lldp](#) 471

[show nmsp](#) 478

[show ptp clock dataset](#) 482

[show ptp clock dataset parent](#) 485

[show ptp clock dataset time-properties](#) 487

[show ptp clock running](#) 489

[show ptp port dataset foreign-master](#) 491

[show ptp port dataset port](#) 493

[shutdown \(bridge-domain\)](#) 495

[snmp-server enable traps ethernet cfm alarm](#) 496

[snmp-server enable traps ethernet cfm cc](#) 497

[snmp-server enable traps ethernet cfm crosscheck](#) 501

[snmp-server enable traps ethernet evc](#) 504

[snmp-server enable traps ether-oam](#) 505

[snmp-server host traps evc](#) 506

[source template \(eoam\)](#) 507

[status decoupled](#) 509

[status peer topology dual-homed](#) 511

[sync interval](#) 513

[template \(eoam\)](#) 515

[timer \(Ethernet ring\)](#) 517

[tod](#) 518

[traceroute ethernet](#) 520

[traceroute ethernet evc](#) 524

[traceroute ethernet vlan](#) 526

[transport ipv4 \(PTP\)](#) 528

[uni count](#) 530

[weight \(srvs instance\)](#) 532



## ais through ethernet cfm logging

---

- [ais, page 3](#)
- [action switch ring g8032 clear instance, page 5](#)
- [action switch ring g8032 instance, page 7](#)
- [alarm, page 9](#)
- [announce interval, page 11](#)
- [announce timeout, page 13](#)
- [aps-channel, page 14](#)
- [backbone interface, page 15](#)
- [bridge-domain \(global\), page 16](#)
- [bridge-domain \(service instance\), page 18](#)
- [bridge-domain from-encapsulation, page 21](#)
- [cfm encapsulation, page 23](#)
- [cfm mep domain, page 25](#)
- [channel-group \(interface\), page 28](#)
- [clear bridge-domain mac-table, page 34](#)
- [clear ethernet cfm ais, page 36](#)
- [clear ethernet cfm errors, page 39](#)
- [clear ethernet cfm maintenance-points remote, page 42](#)
- [clear ethernet cfm statistics, page 44](#)
- [clear ethernet cfm traceroute-cache, page 45](#)
- [clear ethernet event microwave data, page 46](#)
- [clear ethernet event microwave statistics, page 47](#)
- [clear ethernet lmi statistics, page 48](#)
- [clear ethernet oam statistics, page 50](#)

- [clear ethernet ring g8032 statistics, page 52](#)
- [clear ethernet service instance, page 53](#)
- [clear lldp, page 55](#)
- [clock destination, page 57](#)
- [clock-port, page 58](#)
- [clock source \(PTP\), page 60](#)
- [continuity-check, page 61](#)
- [cos \(CFM\), page 63](#)
- [delay-req interval, page 64](#)
- [description \(Ethernet ring\), page 66](#)
- [description \(mac-tunnel\), page 67](#)
- [disable \(CFM-AIS-link\), page 68](#)
- [encapsulation dot1ah isid, page 69](#)
- [errdisable recovery cause mac-security, page 70](#)
- [errdisable recovery cause mlacp-minlink, page 72](#)
- [ethernet cfm ais, page 73](#)
- [ethernet cfm ais link-status, page 75](#)
- [ethernet cfm ais link-status global, page 77](#)
- [ethernet cfm alarm, page 78](#)
- [ethernet cfm cc, page 80](#)
- [ethernet cfm cc enable level evc, page 84](#)
- [ethernet cfm cc enable level vlan, page 86](#)
- [ethernet cfm distribution enable, page 89](#)
- [ethernet cfm domain level, page 90](#)
- [ethernet cfm enable \(interface\), page 92](#)
- [ethernet cfm enable, page 93](#)
- [ethernet cfm global, page 94](#)
- [ethernet cfm ieee, page 95](#)
- [ethernet cfm interface, page 96](#)
- [ethernet cfm logging, page 97](#)

# ais

To enable the Alarm Indication Signal (AIS) function for a specific maintenance association, use the **ais** command in Ethernet connectivity fault management (CFM) service configuration mode. To disable AIS configuration, use the **no** form of this command.

**ais** [**expiry-threshold** *threshold*] **level** *level-id* [**period** *seconds*] **suppress-alarms**

**no ais** [**expiry-threshold** | **level** | **period** | **suppress-alarms**]

## Syntax Description

<b>expiry-threshold</b>	(Optional) Configures the expiry threshold.
<i>threshold</i>	(Optional) Integer from 2 to 255 that is a count. If no MEPs are received within an interval of the threshold multiplied by the transmission period, the MEP clears the AIS defect condition. The default is 3.5.
<b>level</b>	(Optional) Indicates a maintenance level where AIS frames for maintenance endpoints (MEPs) belonging to the service will be sent.
<i>level-id</i>	(Optional) Integer from 0 to 7 that identifies the maintenance level.
<b>period</b>	(Optional) Configures the AIS transmission period for all MEPs in the maintenance association.
<i>seconds</i>	(Optional) Integer value 1 or 60 that indicates the AIS transmission period in seconds. The default is 60.
<b>suppress-alarms</b>	(Optional) Configures alarm suppression.

## Command Default

The AIS function is enabled on specific maintenance associations.

## Command Modes

Ethernet CFM service configuration (config-ecfm-srv)

## Command History

Release	Modification
15.0(1)XA	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Release	Modification
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.
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

Alarms are suppressed when a MEP goes into an RX AIS (receipt of an AIS frame) defect condition.

When you specify the **level** keyword with the **ais** command, you can transmit AIS messages to a higher maintenance association without configuring a maintenance intermediate point (MIP) for that maintenance association.

Output of the **show running all** command shows “ais expiry-threshold 3.5” when the default expiry threshold is configured, “ais period 60” when the default transmission period is configured, and “no ais suppress-alarms” when the default value for the **suppress-alarms** option is configured.

### Examples

The following example shows how to enable the AIS function at level 5 with a transmission period of one second:

```
Device(config)# ethernet cfm domain operatorA level 5
Device(config-ecfm)# service vlan-id 10 port
Device(config-ecfm-srv)# ais period 1
Device(config-ecfm-srv)# ais level 5
```

### Related Commands

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

## action switch ring g8032 clear instance

To specify the action of clearing a signal degradation (SD) occurrence on a link of a G.8032 Ethernet Protection Ring (ERP) topology, use the **action switch ring g8032 clear instance** command in applet configuration mode. To delete this action, use the **no** form of this command.

**action** *action-id* **switch ring g8032 clear** *ring-name* **instance** {*instance-id* | **all**}

**no action** *action-id*

### Syntax Description

<i>action-id</i>	Action identifier. Associates the identifier with the protocol switch action.
<i>ring-name</i>	Name of the G.8032 ERP ring.
<i>instance-id</i>	Instance identifier.
<b>all</b>	Indicates that all instances will be cleared.

### Command Default

The action to clear the SD occurrence is not specified.

### Command Modes

Applet configuration (config-applet)

### Command History

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

### Usage Guidelines

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

This action specified by the **action switch ring g8032 clear instance** command clears the SD condition on the specified ring instances and brings the instances back to the normal (idle) state.

### Examples

The following example shows the **action switch ring g8032 clear instance** command in an Ethernet microwave event configuration:

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

**Related Commands**

Command	Description
event manager applet	Registers an applet with the EEM and enters applet configuration mode.



## action switch ring g8032 instance

To specify the protocol switch action for an instance on a link of a G.8032 Ethernet protection ring (ERP) topology, use the **action switch ring g8032 instance** command in applet configuration mode. To delete this action, use the **no** form of this command.

**action** *action-id* **switch ring g8032** *ring-name* **instance** [*instance-id*] **all** [**interface** *type number*]

**no action** *action-id*

### Syntax Description

<i>action-id</i>	Action identifier.
<i>instance-id</i>	Instance identifier. Enter either a 1 or a 2.
<b>all</b>	Indicates that all instances will be cleared.
<b>interface</b> <i>type number</i>	(Optional) Specifies the interface type and number.

### Command Default

The protocol switch action is not specified.

### Command Modes

Applet configuration (config-applet)

### Command History

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

### Usage Guidelines

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

### Examples

The following example shows the **action switch ring g8032 instance** command in an Ethernet microwave event configuration:

```
Device>
Device# configure terminal
Device(config)# event manager applet mw_ring_sd_2
Device(config-applet)# event ethernet microwave sd interface gigabitethernet 0/0/0 threshold
200
Device(config-applet)# action 1 switch ring g8032 ringA instance 1
```

**Related Commands**

Command	Description
event manager applet	Registers an applet with the EEM and enters applet configuration mode.

# alarm

To configure an alarm when fault alarms are enabled, use the **alarm** command in Ethernet connectivity fault management (CFM) interface configuration mode. To remove the configuration, use the **no** form of this command.

**alarm** {**delay** *mseconds*| **notification** {**all**| **error-xcon**| **mac-remote-error-xcon**| **none**| **remote-error-xcon**| **xcon**}| **reset** *mseconds*}

**no alarm** {**delay**| **notification** {**all**| **error-xcon**| **mac-remote-error-xcon**| **none**| **remote-error-xcon**| **xcon**}| **reset**}

## Syntax Description

<b>delay</b>	Sets a delay time value during which one or more defects must be present before a fault alarm is issued.
<i>mseconds</i>	Integer from 2500 to 10000 that specifies the number of milliseconds for either a delay or a reset of an alarm.  The default is 2500 for the <b>delay</b> option. The default is 10000 for the <b>reset</b> option.
<b>notification</b>	Sets the defects that are to be reported if fault alarms are enabled.
<b>all</b>	Reports all defects: DefRDI, DefMACStatus, DefRemote, DefError, and DefXcon.
<b>error-xcon</b>	Reports only DefError and DefXcon defects.
<b>mac-remote-error-xcon</b>	Reports only DefMACStatus, DefRemote, DefError, and DefXcon (default) defects. This option is the default.
<b>none</b>	No defects are reported.
<b>remote-error-xcon</b>	Reports only DefRemote, DefError, and DefXcon defects.
<b>xcon</b>	Reports only DefXcon defects.
<b>reset</b>	Sets a reset time value that, after a fault alarm, no defects must be present before another fault alarm is enabled.

## Command Default

Alarms are disabled.

**Command Modes**

Ethernet CFM interface configuration (config-if-ecfm-mep)

**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**

This command overrides the global **ethernet cfm alarm** command.

If a higher priority defect occurs after a lower priority defect has triggered an alarm but before the alarm has reset, immediately issue another fault alarm for the higher priority defect.

Output of the **show running all** command displays “alarm delay 2500” when the default value for the **delay** option is configured, “alarm mac-remote-error-xcon” when the default value for the **notification** option is configured, and “alarm reset 10000” when the default value for the **reset** option is configured.

**Examples**

The following example shows how to set up notifications for all defects:

```
Device(config)# ethernet cfm domain test level 5
Device(config-ecfm)# service vlan-id 17 vlan 17
Device(config-ecfm-srv)# exit
Device(config-ecfm)# exit
Device(config-if)# ethernet cfm mep domain test mpid 5 vlan 17
Device(config-if-ecfm-mep)# alarm notification all
Device(config-if-ecfm-mep)#
```

The following example shows how to set the time during which one or more defects must be present before a fault alarm is issued to 7000 milliseconds:

```
Device(config)# ethernet cfm domain test level 5
Device(config-ecfm)# service vlan-id 17 vlan 17
Device(config-ecfm-srv)# exit
Device(config-ecfm)# exit
Device(config-if)# ethernet cfm mep domain test mpid 5 vlan 17
Device(config-if-ecfm-mep)# alarm delay 7000
```

**Related Commands**

Command	Description
<b>ethernet cfm alarm</b>	Configures an alarm for Ethernet CFM.
<b>show running all</b>	Shows the running configuration with default values.

# announce interval

To set an interval value for timing announcement packets, use the **announce interval** command in Precision Time Protocol clock port mode. To remove an announcement interval configuration, use the **no** form of this command.

**announce interval** *interval-value*

**no announce interval** *interval-value*

## Syntax Description

<i>interval-value</i>	<p>Specifies the interval for announce messages. The intervals use log base 2 values, as follows:</p> <ul style="list-style-type: none"> <li>• 4--1 packet every 16 seconds</li> <li>• 3--1 packet every 8 seconds</li> <li>• 2--1 packet every 4 seconds</li> <li>• 1--1 packet every 2 seconds</li> <li>• 0--1 packet every second</li> </ul>
-----------------------	---

## Command Default

For the IE 3000 switch, the default value is 1. For the MWR 2941 router, the default value is 2.

## Command Modes

PTP clock port configuration (config-ptp-port)

## Command History

Release	Modification
15.0(1)S	This command was introduced.

## Usage Guidelines

The interval value defined by this command impacts the timeout value defined by the **announce timeout** command.

## Examples

The following example shows how to configure an announcement interval:

```
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# clock-port slave slaveport
Router(config-ptp-port)# announce interval 3
Router(config-ptp-port)# end
Router#
```

**Related Commands**

Command	Description
<b>announce timeout</b>	Sets the timeout value for timing announcement packets.

## announce timeout

To set a timeout value for timing announcement packets, use the **announce timeout** command in Precision Time Protocol clock port mode. To remove an announcement timeout configuration, use the **no** form of this command.

**announce timeout** *timeout-value*

**no announce timeout** *timeout-value*

### Syntax Description

<i>timeout-value</i>	Specifies the number of announcement intervals before the session times out. The range is from 1 to 10. The default is 3.
----------------------	---

### Command Default

The default timeout value is 3.

### Command Modes

PTP clock port configuration (config-ptp-port)

### Command History

Release	Modification
15.0(1)S	This command was introduced.

### Usage Guidelines

This command configures the number of announcement intervals before the session times out. To define the length of the announcement intervals, use the **announce interval** command.

### Examples

The following example shows how to configure an **announcement timeout**:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# announce timeout 7
Device(config-ptp-port)# end
```

### Related Commands

Command	Description
<b>announce interval</b>	Sets interval value for timing announcement packets.

# aps-channel

To enter Ethernet ring instance aps-channel configuration mode, use the **aps-channel** command in Ethernet ring instance configuration mode. To exit Ethernet ring instance aps-channel configuration mode, use the **no** form of this command.

**aps-channel**

**no aps-channel**

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

**Command Default** Ethernet ring instance aps-channel configuration mode is not entered.

**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.

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

**Examples** The following is an example of the **aps-channel** command used in an Ethernet ring configuration.

```
Device> enable
Device# configure terminal
Device(config-config)# ethernet ring g8032 r1
Device(config-erp-ring)# instance 1
Device(config-erp-inst)# aps-channel
Device(config-erp-inst-aps)#
```



# backbone interface

To configure a backbone interface for a redundancy group, use the **backbone interface** command in interchassis redundancy configuration mode. To remove the configuration, use the **no** form of this command.

**backbone interface** *type number*

**no backbone interface** *type number*

## Syntax Description

<i>type</i>	String that identifies the type of interface.
<i>number</i>	Integer that identifies the interface.

## Command Default

A backbone interface is not configured.

## Command Modes

Interchassis redundancy configuration (config-r-ic)

## Command History

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

## Usage Guidelines

Use this command to configure a backbone interface to monitor all interfaces in a redundancy group. For example, if all interfaces are in the DOWN state (core isolation), the backbone interface signals the redundancy group clients, and they may initiate attachment circuit (AC) failover procedures. An example client might be Multichassis Link Aggregation Control Protocol (mLACP).

## Examples

The following example shows how to configure an Ethernet backbone interface:

```
Router> enable
Router# configure terminal
Router(config)# redundancy
Router(config-r)# interchassis group 1
Router(config-r-ic)# backbone interface ethernet 0/1
```

## bridge-domain (global)

To configure components on a bridge domain, use the **bridge-domain** command in global configuration mode. To remove the configured components from the bridge domain and to return the components to the bridge-domain default state, use the **no** form of this command.

**bridge-domain** {*bridge-id* [**c-mac**] **c-mac** **aging-time** *minutes*}

**no bridge-domain** {*bridge-id* [**c-mac**] **c-mac** **aging-time**}

### Syntax Description

<i>bridge-id</i>	Integer from 1 to 16384 that identifies the bridge domain. <ul style="list-style-type: none"><li>The upper limit may vary based on the platform.</li></ul>
<b>c-mac</b>	Configures the bridge domain as a customer domain.
<b>aging-time</b>	Configures the aging time for the customer domain.
<i>minutes</i>	Integer from 1 to 600 that is the aging time, in minutes. The default is 5.

### Command Default

No components are configured on the bridge domain.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(33)SRE	This command was modified. The <b>aging-time</b> and <b>c-mac</b> keywords were added and the <i>minutes</i> argument was added.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S

### Usage Guidelines

When the **bridge-domain** command is executed without the **aging-time** keyword, the command mode changes from global configuration mode (config) to bridge-domain configuration mode (config-bdomain). Issuing the **bridge-domain c-mac aging-time** command does not result in a command mode change.

In bridge-domain configuration mode, additional components can be configured on the bridge domain; for example, the MAC address limiting security component.

**Note**

In service instance configuration mode, the **bridge-domain** command binds a service instance to a bridge-domain instance.

**Examples**

The following example shows how to configure a bridge domain as a customer domain and place the CLI in bridge-domain configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# bridge-domain 100 c-mac
Device(config-bdmain)# mac limit maximum addresses 10
```

The following example shows how to configure a bridge domain as a customer domain with an aging time of 400 minutes:

```
Device> enable
Device# configure terminal
Device(config)# bridge-domain c-mac aging-time 400
Device(config)#
```

**Related Commands**

Command	Description
<b>bridge-domain</b>	In service instance configuration mode, binds a service instance to a bridge domain.
<b>mac limit maximum addresses</b>	Specifies the MAC address limit on a bridge domain.

## bridge-domain (service instance)

To bind a service instance or a MAC tunnel to a bridge domain instance, use the **bridge-domain** command in either service instance configuration mode or MAC-in-MAC tunnel configuration mode. To unbind a service instance or MAC tunnel from a bridge domain instance, use the **no** form of this command.

**bridge-domain** *bridge-id* [**split-horizon** [**group** *group-id*]]

**no bridge-domain** *bridge-id* [**split-horizon** [**group** *group-id*]]

### Syntax on the Cisco ASR 1000 Series Aggregation Device

**bridge-domain** *bridge-id* [**split-horizon** **group** *group-id*]

**no bridge-domain** *bridge-id* [**split-horizon** **group** *group-id*]

### Syntax Description

<i>bridge-id</i>	Numerical identifier for the bridge domain instance. The range is an integer from 1 to the platform-specific maximum (or upper) limit. <ul style="list-style-type: none"> <li>The upper limit on the Cisco ASR 1000 device is 4096.</li> </ul>
<b>split-horizon</b>	(Optional) Configures a port or service instance as a member of a split-horizon group. <ul style="list-style-type: none"> <li>This keyword is not supported in MAC-in-MAC tunnel configuration mode.</li> </ul>
<b>group</b>	(Optional) Defines the split-horizon group. <ul style="list-style-type: none"> <li>This keyword is not supported in MAC-in-MAC tunnel configuration mode.</li> </ul>
<i>group-id</i>	(Optional) Identifier for the split-horizon group. Range is 1 to 65533. <ul style="list-style-type: none"> <li>This argument is not supported in MAC-in-MAC tunnel configuration mode.</li> <li>On the Cisco ASR 1000 device, the only values supported are <b>0</b> and <b>1</b>.</li> </ul>

### Command Default

Service instances and MAC tunnels are not bound to a bridge domain instance.

### Command Modes

Service instance configuration (config-if-svc)

MAC-in-MAC tunnel configuration (config-tunnel-minm)

### Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SRD	This command was modified. The <b>split-horizon</b> keyword was added.
12.2(33)SRE	This command was modified. Support for this command was added in MAC-in-MAC tunnel configuration mode.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

### Usage Guidelines

Use the **bridge-domain**(service instance) command to bind either a service instance or a MAC tunnel to a bridge domain.

Bridge domains cannot be configured under a service instance under a MAC tunnel without encapsulation also being configured.

The Cisco ASR 1000 device does not support MAC tunnels.



#### Note

The **bridge-domain**(config) command allows a user to configure components on a bridge domain. For example, the MAC Address Limiting security component can be configured on a bridge domain using this command.

### Examples

The following example shows how to bind a bridge domain to a service instance:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1q 100
Device(config-if-srv)# bridge-domain 200
```

The following example shows how to bind a MAC tunnel to a service instance:

```
Device> enable
Device# configure terminal
Device(config)# ethernet mac-tunnel virtual 100
Device(config-tunnel-minm)# bridge-domain 200
```

### Related Commands

Command	Description
<b>bridge-domain (config)</b>	Enables a user to configure components on a bridge domain.

Command	Description
<b>ethernet evc</b>	Defines an EVC and enters EVC configuration mode.
<b>ethernet service instance</b>	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
<b>encapsulation dot1ad</b>	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance. The criteria for this command are single VLAN, range of VLANs, and lists of these two criteria.
<b>encapsulation dot1q</b>	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
<b>encapsulation dot1q second dot1q</b>	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
<b>encapsulation untagged</b>	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

# bridge-domain from-encapsulation

To create a range of bridge domains on the basis of the bridge-domain IDs derived from encapsulation VLAN numbers, use the **bridge-domain from-encapsulation** command in Ethernet service configuration mode. To remove the bridge domains, use the **no** form of this command.

**bridge-domain from-encapsulation**

**no bridge-domain from-encapsulation**

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

**Command Default** Bridge domains are not created.

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

Command History	Release	Modification
	Cisco IOS XE Release 3.5S	This command was introduced.

**Usage Guidelines** Use the **bridge-domain from-encapsulation** command in Ethernet service configuration mode (config-if-srv) to configure support for Ethernet Flow Points (EFPs) on trunk ports (interfaces).

To enter Ethernet service configuration mode (config-if-srv), use the **service instance ethernet** command.

The **bridge-domain from-encapsulation** command is used in conjunction with the **encapsulation dot1q** command. The **bridge-domain from-encapsulation** command uses the VLAN range specified by the **encapsulation dot1q** command to create the corresponding range of bridge domains. In the following example, bridge domains in the range of 12 to 1900 are created on the basis of the VLAN range specified by the **encapsulation dot1q** command.

```
Router(config)# interface GigabitEthernet0/0/5
Router(config-if)# service instance trunk 4000 ethernet
Router(config-if-srv)# encapsulation dot1q 12-1900
Router(config-if-srv)# bridge-domain from-encapsulation
```

**Examples** The following is an example of the **bridge-domain from-encapsulation** command in a typical configuration:

```
Router(config)# interface gigabitethernet2/0/1
Router(config-if)# service instance trunk 1 ethernet
Router(config-if-srv)# encapsulation dot1q 1 - 5, 7, 9-12
Router(config-if-srv)# bridge-domain from-encapsulation
```

**Related Commands**

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



# cfm encapsulation

To configure connectivity fault management (CFM) Ethernet frame encapsulation, use the **cfm encapsulation** command in service instance configuration mode. To remove the encapsulation, use the **no** form of this command.

**cfm encapsulation** {**dot1ad** *vlan-id*| **dot1q** *vlan-id*} [**cos** *cos-value*] [**dot1q** *vlan-id*| **second-dot1q** *vlan-id*] [**cos** *cos-value*]

**no cfm encapsulation** {**dot1ad** *vlan-id*| **dot1q** *vlan-id*} [**cos** *cos-value*] [**dot1q** *vlan-id*| **second-dot1q** *vlan-id*] [**cos** *cos-value*]

## Syntax Description

<b>dot1ad</b>	Indicates the 802.1ad provider bridges encapsulation type.
<i>vlan-id</i>	Integer from 1 to 4094 that specifies the VLAN on which to send CFM frames.
<b>dot1q</b>	(Optional) Supports the IEEE 802.1q standard for encapsulation of traffic and specifies the outer dot1q encapsulation tag.
<b>cos</b>	(Optional) Indicates the class of service (CoS) for CFM packets.
<i>cos-value</i>	(Optional) Integer from 0 to 7 that specifies the CoS.
<b>second-dot1q</b>	(Optional) Specifies the inner dot1q encapsulation tag. Valid option only when you first select the outer <b>dot1q</b> encapsulation tag. When the <b>dot1ad</b> encapsulation type is selected first, <b>dot1q</b> is a valid option.

**Command Default** CFM Ethernet frame encapsulation is not configured.

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

## Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Release	Modification
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S and was modified for use with the Cisco ASR 903 Router. For more information, see “Usage Guidelines.”

### Usage Guidelines

To use the **cfm encapsulation** command, you must first use the **bridge-domain** command in Ethernet service configuration mode to configure a bridge domain.



#### Note

On the Cisco ASR 903 Router, you do *not* need to first use the **bridge-domain** command to configure a bridge domain. For the Cisco ASR 903 router, configuring a bridge domain is not a prerequisite.

When a range of VLANs is configured under the Ethernet flow point, the **cfm encapsulation** command configures the VLAN ID on which to send locally sourced CFM frames. The VLAN ID specified must be within the range configured in the **encapsulation** command.

The **cfm encapsulation** command does not support untagged service instances.

### Examples

The following example shows how to configure the **cfm encapsulation** command:

```

ethernet cfm domain CUSTOMER level 7 direction outward
 service customer_100 evc evc_100
ethernet cfm domain MIP level 7
ethernet cfm domain PROVIDER level 4
 service provider_100 evc evc_100
 mep crosscheck mpid 200 evc evc_100 mac aabb.cc00.0310
ethernet evc evc_100
interface Ethernet 1/0
 no ip address
 service instance 100 ethernet evc_100
 encapsulation dot1q 100
 bridge-domain 100
 cfm encapsulation dot1q 1 cos 2 second-dot1q 3 cos 4

```

### Related Commands

Command	Description
<b>bridge-domain</b>	Binds a service instance to a bridge domain instance.
<b>encapsulation</b>	Sets the encapsulation method used by the interface.
<b>service instance ethernet</b>	Configures an Ethernet service instance on an interface and places the CLI in service instance configuration mode.

## cfm mep domain

To configure a maintenance endpoint (MEP) for a domain, use the **cfm mep domain** command in either service instance configuration mode or virtual forwarding instance (VFI) configuration mode. To remove the MEP, use the **no** form of this command.

**cfm mep domain** *domain-name* [**inward**| **outward**] **mpid** *mpid-value* [**cos** *cos-value*]

**no cfm mep domain** *domain-name* [**inward**| **outward**] **mpid** *mpid-value*

### Syntax Description

<i>domain-name</i>	String from 1 to 154 characters that identifies the domain name.
<b>inward</b>	(Optional) Indicates inward direction of connectivity fault management (CFM) packets.
<b>outward</b>	(Optional) Indicates outward direction of CFM packets.
<b>mpid</b>	Indicates the maintenance point ID (MPID).
<i>mpid-value</i>	Integer from 1 to 8191 that identifies the MPID.
<b>cos</b>	(Optional) Indicates the class of service (CoS) for CFM packets.
<i>cos-value</i>	(Optional) Integer from 0 to 7 that specifies the CoS.

### Command Default

A MEP for a domain is not configured.

### Command Modes

Service instance configuration (config-if-srv)  
VFI configuration (config-vfi)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S and was modified for use with the Cisco ASR 903 Router. For more information, see "Usage Guidelines."

## Usage Guidelines

The **cfm mep domain** command defines an Ethernet flow point as an MEP. To use the **cfm mep domain** command, you must first configure a bridge domain in service instance configuration mode by issuing the **bridge-domain** command.



### Note

On the Cisco ASR 903 Router, you do *not* need to first issue the **bridge-domain** command. The MEP is not operational until you associate the bridge domain with the service instance. To establish the association between the bridge domain and the service instance, either configure the **bridge-domain** command under the service instance or use the **member** command in global configuration mode as shown below. The MEP becomes nonoperational if the bridge domain is later disassociated with the service instance.

```

ethernet cfm domain CUSTOMER level 6
service customer_100 evc evc100 vlan 100
!
ethernet evc evc100
!
bridge-domain 100
member interface Ethernet0/0 service instance 100
!
interface Ethernet0/0
service instance 100 ethernet evc100
 encapsulation dot1q 100
 cfm mep domain CUSTOMER mpid 1001

```

To verify whether the bridge domain is associated with the service instance, use the **show ethernet cfm maintenance-points local** command.

Device# **show ethernet cfm maintenance-points local**

Local MEPs:

MPID	Domain Name	Lvl	MacAddress	Type	CC
Ofld	Domain Id	Dir	Port	Id	
	MA Name		SrvInst	Source	
	EVC name				
1001	CUSTOMER	6	aabb.cc00.0199	BD-V	I
No	null	Up	Et0/0	0	
	customer_100		100	Static	
	evc100				

If the bridge domain is not associated with the service instance, the continuity check (CC) operational status is "I" for Inactive and the Id value is "0".

## Examples

The following example shows how to configure the **cfm mep domain** command:

```

ethernet cfm domain CUSTOMER level 7 direction outward
service customer_100 evc evc_100
ethernet cfm domain MIP level 7
ethernet cfm domain PROVIDER level 4
service provider_100 evc evc_100
mep crosscheck mpid 200 evc evc_100 mac aabb.cc00.0310
ethernet evc evc_100
interface Ethernet 1/0
no ip address
service instance 100 ethernet evc_100
 encapsulation dot1q 100
 bridge-domain 100
 cfm mep domain CUSTOMER outward mpid 1001

```

**Related Commands**

Command	Description
<b>bridge-domain</b>	Binds the service instance to a bridge domain instance.
<b>member</b>	Specifies the two members of the Virtual Private Wire Service (VPWS), multisegment pseudowire, or local connect services.
<b>service instance ethernet</b>	Configures an Ethernet service instance on an interface and places the CLI in service instance configuration mode.
<b>show ethernet cfm maintenance-points local</b>	Displays information about maintenance points configured on a device.

## channel-group (interface)

To assign and configure an EtherChannel interface to an EtherChannel group, use the **channel-group** command in interface configuration mode. To remove the channel-group configuration from the interface, use the **no** form of this command.

**channel-group** *channel-group-number* **mode** {**active**|**on**|**passive**}  
**no channel-group** *channel-group-number*

### Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

**channel-group** *channel-group-number* **mode on**  
**no channel-group** *channel-group-number*

### Cisco ASR 1000 Series Routers

**channel-group** *channel-group-number* **mode** {**active**|**passive**}  
**no channel-group**

### Cisco Catalyst Switches

**channel-group** *channel-group-number* **mode** {**active**|**on**|**auto** [**non-silent**]|**desirable** [**non-silent**]|**passive**}  
**no channel-group** *channel-group-number*

### Syntax Description

<i>channel-group-number</i>	Integer that identifies the channel-group. Valid values are from 1 to 256; the maximum number of integers that can be used is 64.  <ul style="list-style-type: none"> <li>For Fast EtherChannel groups, the number is an integer from 1 to 4. This number is the one previously assigned to the port-channel interface.</li> <li>On the Cisco ASR 1000 series router, valid values are from 1 to 64.</li> </ul>
<b>mode</b>	Specifies the EtherChannel mode of the interface.
<b>active</b>	Enables Link Aggregation Control Protocol (LACP) unconditionally.
<b>on</b>	Enables EtherChannel only.
<b>auto</b>	Places a port into a passive negotiating state in which the port responds to Port Aggregation Protocol (PAgP) packets that it receives but does not initiate PAgP packet negotiation.

<b>non-silent</b>	(Optional) Used with the <b>auto</b> or <b>desirable</b> mode when traffic is expected from the other device.
<b>desirable</b>	Places a port into an active negotiating state in which the port initiates negotiations with other ports by sending PAgP packets.
<b>passive</b>	Enables LACP only when an LACP device is detected. This is the default state.

**Command Default** No channel groups are assigned.

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.1CA	This command was introduced.
	12.0(7)XE	Support for this command was implemented on Cisco Catalyst 6000 series switches.
	12.1(3a)E3	The number of valid values for the <i>number</i> argument was changed; see the "Usage Guidelines" section for valid values.
	12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	Support for this command was implemented on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 3700 series routers and integrated into Cisco IOS Release 12.2(8)T .
	12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
	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(18)SXE	This command was changed to support advanced QinQ translation on QinQ link bundles using GE-WAN interfaces on an OSM-2+4GE-WAN+ OSM on Cisco 7600 series routers.
	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.

Release	Modification
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

## Usage Guidelines

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

### IP Address for the Physical Interface

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but Cisco highly recommends doing so.

### Layer 2 and Layer 3 Port Channels

You can create both Layer 2 and Layer 3 port channels by entering the **interface port-channel** command or, when the channel-group gets its first physical interface assignment. The port channels are not created at run time, nor are they created dynamically.

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is automatically created when the channel group gets its first physical interface, if it is not already created.

### Propagation of Configuration and Attribute Changes

Any configuration or attribute changes you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel. (for example, configuration changes are also propagated to the physical interfaces that are not part of the port-channel, but are part of the channel group.)

### The on Keyword

When you use the **on** keyword, a usable EtherChannel exists only when a port group in on mode is connected to another port group in the on mode.

### Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

### Cisco ASR 1000 Series Routers

The Cisco ASR 1000 series router has the following prerequisites and restriction:

- A port-channel must be created before member links are assigned to it.
- IP addresses must be disabled on member links before those links can be included in a port-channel.
- Fast Ethernet interfaces are not supported.

### Cisco Catalyst Switches

The number of valid values for *number* depends on the software release. For software releases prior to Cisco IOS Release 12.1(3a)E3, valid values are from 1 to 256; for Cisco IOS Release 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Cisco IOS Release 12.1 E and later releases support a maximum of 64 values ranging from 1 to 256.

The channel-group number is global and is shared between all the channeling protocols. If a specific channel number is used for the PAgP-enabled interfaces of a channel group, that same channel number cannot be used for configuring a channel that has LACP-enabled interfaces or vice versa.



Entering the **auto** or **desirable** keyword enables PAgP on the specified interface; the command will be rejected if it is issued on an LACP-enabled interface.

The **active** and **passive** keywords are valid on PAgP-disabled interfaces only.

You can change the mode for an interface only if it is the only interface that is designated to the specified channel group.

The **on** keyword forces the bundling of the interface on the channel without any negotiation.

You can manually configure a switch with PAgP on one side and LACP on the other side in the **on** mode.

With the **on** mode, a usable EtherChannel exists only when a port group in **on** mode is connected to another port group in **on** mode.

If you enter the **channel group** command on an interface that is added to a channel with a different protocol than the protocol you are entering, the command is rejected.

If the interface belongs to a channel, the **no** form of this command is rejected.

All ports in the same channel group must use the same protocol; you cannot run two protocols on one channel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol.

Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).

All ports in a channel must be on the same DFC-equipped module. You cannot configure any of the ports to be on other modules.

On systems that are configured with nonfabric-enabled modules and fabric-enabled modules, you can bundle ports across all modules, but those bundles cannot include a DFC-equipped module port.

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but it is highly recommended.

You can create both Layer 2 and Layer 3 port channels by entering the **interface port-channel** command or when the channel group gets its first physical interface assignment. The port channels are not created at runtime or dynamically.

Any configuration or attribute changes that you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel but are part of the channel group).

When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port-channel logical interfaces.

Only the **on** mode is supported when using this command with GE-WAN ports on the OSM-2+4GE-WAN+ OSM to create QinQ link bundles for advanced QinQ translation. Also, you cannot use the **channel-group** command on GE-WAN interfaces if MPLS is configured. You must remove all IP, MPLS, and other Layer 3 configuration commands before using the **channel-group** command with GE-WAN interfaces.

**Note**

The GE-WAN interfaces on an OSM-2+4GE-WAN+ OSM behave slightly differently than other interfaces if you want to move the interface from one group to another. To move most other interfaces, you can enter the **channel-group** command again to delete the interface from the old group and move it to the new group. For GE-WAN ports, however, you must manually remove the interface from the group by entering the **no channel-group** command before assigning it to a new group.

**Caution**

Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Assigning bridge groups on the physical EtherChannel interfaces causes loops in your network.

For a complete list of guidelines, see the “Configuring EtherChannel” section of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

**Fast EtherChannel**

Before you assign a Fast Ethernet interface to a Fast EtherChannel group, you must first create a port-channel interface. To create a port-channel interface, use the **interface port-channel** global configuration command.

If the Fast Ethernet interface has an IP address assigned, you must disable it before adding the Fast Ethernet interface to the Fast EtherChannel. To disable an existing IP address on the Fast Ethernet interface, use the **no ip address** command in interface configuration mode.

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. Fast EtherChannel can be configured between Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) or between a Cisco 7500 series router or a Cisco 7000 series router with the RSP7000 and RSP700CI and a Cisco Catalyst 5000 switch.

A maximum of four Fast Ethernet interfaces can be added to a Fast EtherChannel group.

**Caution**

The port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces. Do not assign bridge groups on the physical Fast Ethernet interfaces because it creates loops. Also, you must disable spanning tree.

To display information about the Fast EtherChannel, use the **show interfaces port-channelEXEC** command.

For more guidelines see the “Configuring EtherChannel” section of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* and the “Configuring EtherChannel” section of the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*

**Examples**

This example shows how to add EtherChannel interface 1/0 to the EtherChannel group that is specified by port-channel 1:

```
Router(config-if) #
channel-group 1 mode on
Router(config-if) #
```

The following example shows how to add interface Fast Ethernet 1/0 to the Fast EtherChannel group specified by port-channel 1:

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

```
exit
Router(config)#
interface fastethernet 1/0
Router(config-if)#
channel-group 1
```

**Related Commands**

Command	Description
<b>interface</b>	Creates a port-channel virtual interface and puts the CLI in interface configuration mode when the <b>port-channel</b> keyword is used.
<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.

# clear bridge-domain mac-table

To clear a bridge domain of learned MAC addresses, use the **clear bridge-domain mac-table** command in privileged EXEC mode.

**clear bridge-domain** *bridge-id* **mac-table** [ *mac-address* ]

## Syntax Description

<i>bridge-id</i>	Integer from 1 to 16384 that identifies a bridge domain.
<i>mac-address</i>	(Optional) MAC address to be cleared.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S

## Usage Guidelines

Use the **clear bridge-domain mac table** command to purge MAC addresses that have been dynamically learned by a bridge domain.

This command is available on both route processors and linecards. To invoke this command use the **remote command module** command; for example, **remote command module 10 clear bridge-domain 25 mac-table**.

## Examples

The following example shows how to clear all dynamically learned MAC addresses in the MAC table of bridge domain 12:

**Device# clear bridge-domain 12 mac table**

The following example shows how to clear a specific MAC address from the MAC table of bridge domain 12:

```
Device#
clear bridge-domain 12 mac table 0001.0001.aaaa
```

**Related Commands**

Command	Description
show bridge-domain	Displays information about a bridge domain.

## clear ethernet cfm ais

To clear a maintenance endpoint (MEP) or server maintenance endpoint (SMEP) from the Ethernet Connectivity Fault Management (CFM) Alarm Indication Signal (AIS) defect condition, use the **clear ethernet cfm ais** command in privileged EXEC mode.

### CFM Cisco Proprietary Draft 8 (CFM D8)

**clear ethernet cfm ais** {**domain** *domain-name* **mpid** *mpid-id* [**evc** *name*] **port** | **vlan** *vlan-id*} [**link-status** **interface** *Ethernet number*]

### Ethernet CFM IEEE 802.1ag Standard (CFM IEEE)

**clear ethernet cfm ais** {**domain** *domain-name* **mpid** *mpid-id* **vlan** *vlan-id*] **link-status** **interface** *Ethernet number*}

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

**clear ethernet cfm ais** {**domain** *domain-name* **service** {*short-ma-name* | **icc** *icc-code* *meg-id*} **number** *ma-number* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**link-status** **interface** *Ethernet number*]

### Syntax Description

<b>domain</b> <i>domain-name</i>	Indicates that a maintenance domain is specified. Specifies a string of a maximum of 154 characters in length that identifies the domain.
<b>mpid</b> <i>mpid</i>	Specifies a MEP identifier (MPID) and value. Range: 1 to 8191.
<b>evc</b> <i>evc-name</i>	String that associates an Ethernet virtual connection (EVC) to the service instance. Maximum: 100 bytes.
<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>link-status</b>	Indicates either an SMEP or a link up/link down condition.
<b>interface</b>	Indicates that an interface is specified.
<b>Ethernet</b> <i>number</i>	Specifies an Ethernet interface. Range: 0 to 15.
<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 (#)

**Command History**

Release	Modification
12.2(33)SRD	This command was introduced.
15.0(1)XA	This command was modified. The <b>evc</b> keyword and <i>name</i> argument were not supported in Cisco IOS Release 15.0(1)XA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.7S	This command was modified. The <b>evc</b> , <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.

**Usage Guidelines**

If an MEP does not exit the AIS state when all errors are resolved, use the **clear ethernet cfm ais** command with the **domain** and **mpid** keywords to clear the AIS defect condition. If an SMEP does not exit the AIS state when all errors are resolved, use the **clear ethernet cfm ais** command with the **link-status interface** keywords to clear the AIS defect condition.

**Examples**

The following example shows how to clear an SMEP of an AIS defect condition:

```
Device# clear ethernet cfm ais link-status interface ethernet 0/0
```

The following example shows how to clear an MEP of an AIS defect condition:

```
Device# clear ethernet cfm ais domain cisco.com mpid 100 service zzz
```

**Related Commands**

Command	Description
ethernet cfm ais	Enables AIS generation from an SMEP.



# clear ethernet cfm errors

To clear continuity check error conditions logged on a device, use the **clear ethernet cfm errors** command in privileged EXEC mode.

## Cisco Pre-Standard Connectivity Fault Management Draft 1.0 (CFM D1)

**clear ethernet cfm errors** [**domain** *domain-name* | **level** *level-id*]

## CFM IEEE 802.1ag Standard (CFM IEEE) and Cisco ASR 901 Series Aggregation Services Router

**clear ethernet cfm errors** [**domain-id** {*mac-address* *domain-number* | *domain-name* | **dns** *dns-name* | **null**}] [**service** {**icc** *icc-code* *meg-code* | *maintenance-association-name* | *maintenance-association-number* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*}]

### Syntax Description

<b>domain</b>	(Optional) Clears errors for a maintenance domain.
<i>domain-name</i>	(Optional) String of a maximum length of 154 characters.
<b>level</b>	(Optional) Clears errors for a maintenance level.
<i>level-id</i>	(Optional) Integer from 0 to 7 that identifies the maintenance level.
<b>domain-id</b>	(Optional) Clears errors by domain ID.
<i>mac-address</i>	MAC address of the maintenance domain.
<i>domain-number</i>	Integer from 0 to 65535 that identifies the maintenance domain.
<b>dns</b>	Specifies a domain name service (DNS).
<i>dns-name</i>	String of a maximum length of 43 characters.
<b>null</b>	Indicates there is not a domain name.
<b>service</b>	(Optional) Specifies a maintenance association within the domain.
<b>icc</b>	Clears error conditions on the basis of the ITU-T Y.1731 Carrier Code (ICC)-based maintenance entity group (MEG) identifier.
<i>icc-code</i>	String that identifies the ICC. String of a maximum of 6 characters.

<i>meg-code</i>	String that identifies the unique MEG code. String of a maximum of 12 characters.
<i>maintenance-association-name</i>	String that identifies the maintenance association.
<i>maintenance-association-number</i>	Integer that identifies the maintenance association.
<b>vlan-id</b>	Specifies a VLAN.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the VLAN.
<b>vpn-id</b>	Specifies a virtual private network (VPN).
<i>vpn-id</i>	Integer from 1 to 32767 that identifies the VPN.

**Command Default**

The error database is unchanged; existing entries remain in the database.

**Command Modes**

Privileged EXEC (#)

**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.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The <b>icc</b> keyword was added to provide support for the ICC-based MEG identifier.
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.
15.3(2)S	This command was implemented on Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines**

Use the **clear ethernet cfm errors** command to purge error database entries that are not needed and when you want to work with a cleared database. Also, use this command with a specified domain if you want to clear errors for that domain.

In CFM IEEE, if a domain name is more than 43 characters in length, 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.

### Examples

The following example shows how to clear errors at maintenance level 3. No output is generated when this command is issued.

```
Device# clear ethernet cfm errors level 3
```

The following example shows how to clear errors for a DNS on VLAN 17. No output is generated when this command is issued.

```
Device# clear ethernet cfm errors domain-id dns Service10 service vlan-id 17
```

### Related Commands

Command	Description
<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.

# clear ethernet cfm maintenance-points remote

To purge the contents of the continuity check database, use the **clear ethernet cfm maintenance-points remote** command in privileged EXEC mode.

## Cisco pre-Standard Connectivity Fault Management Draft 1.0 (CFM D1)

**clear ethernet cfm maintenance-points remote** [**domain** *domain-name*] [**level** *level-id*]

## CFM IEEE 802.1ag Standard (CFM IEEE)

**clear ethernet cfm maintenance-points remote** [**domain** *domain-name*]

### Syntax Description

<b>domain</b>	(Optional) Indicates that a maintenance domain is specified.
<i>domain-name</i>	(Optional) String of a maximum of 154 characters that identifies the domain.
<b>level</b>	(Optional) Indicates that a maintenance level is specified. <ul style="list-style-type: none"><li>• This keyword is not available in CFM IEEE.</li></ul>
<i>level-id</i>	(Optional) Integer in the range of 0 to 7 that identifies the maintenance level. <ul style="list-style-type: none"><li>• This argument is not available in CFM IEEE.</li></ul>

### Command Default

The continuity check database is unchanged; existing entries remain in the database.

### Command Modes

Privileged EXEC (#)

### 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.

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

### Usage Guidelines

Use this command to clear the entire continuity check database or clear the database for a specific domain or level. When a domain is specified, only entries for that domain are purged. When a level is specified, entries for all domains at that level are purged.

If a maintenance domain is not specified, the entire continuity check database is cleared.

In CFM IEEE, the **level** keyword and *level-id* argument are not supported. Also, if a domain name is 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.

### Examples

The following example shows how to purge the contents of the continuity check database. No output is generated when this command is issued.

```
Device# clear ethernet cfm maintenance-points remote
```

### Related Commands

Command	Description
<b>show ethernet cfm maintenance-points remote</b>	Displays information about remote maintenance points in the continuity check database.

## clear ethernet cfm statistics

To clear a maintenance endpoint (MEP) or server maintenance endpoint (SMEP) out of the Alarm Indication Signal (AIS) defect condition, use the **clear ethernet cfm ais** command in privileged EXEC mode.

**clear ethernet cfm statistics** [*mpid mpid-id*]

### Syntax Description

<b>mpid</b>	Indicates that a maintenance point ID (MPID) is specified.
<i>mpid-id</i>	An integer in the range of 1 to 8191 that identifies the MPID.

### Command Modes

Privileged EXEC (#)

### 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.

### Usage Guidelines

If a MEP does not exit the AIS state when all errors are resolved, use the **clear ethernet cfm ais** command with the **domain** and **mpid** keywords to clear the AIS defect condition. If a SMEP does not exit the AIS state when all errors are resolved, use the **clear ethernet cfm ais** command with the **link-status interface** keywords to clear the AIS defect condition.

### Examples

The following example shows how to clear connectivity fault management (CFM) statistics from a SMEP of an AIS defect condition:

```
Device# clear ethernet cfm statistics mpid 800
```

### Related Commands

Command	Description
<b>clear ethernet cfm ais</b>	Clears a MEP or SMEP out of the AIS defect condition.

# clear ethernet cfm traceroute-cache

To remove the contents of the traceroute cache, use the **clear ethernet cfm traceroute-cache** command in privileged EXEC mode.

**clear ethernet cfm traceroute-cache**

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

**Command Modes** Privileged EXEC (#)

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** Use the **clear ethernet cfm traceroute-cache** command to remove traceroute cache entries from previous traceroute operations issued on the device. This command also provides visibility into maintenance intermediate points and maintenance endpoints of a domain as they were recorded when the operation was performed.

**Examples** The following example shows how to remove the contents of the traceroute cache:

```
Device# clear ethernet cfm traceroute-cache
```

Related Commands	Command	Description
	<b>ethernet cfm traceroute cache</b>	Enables caching of Ethernet CFM data learned through traceroute messages.
	<b>show ethernet cfm traceroute-cache</b>	Displays the contents of the traceroute cache.

# clear ethernet event microwave data

To clear Ethernet microwave event data for one or more interfaces, use the **clear ethernet event microwave data** command in privileged EXEC mode.

**clear ethernet event microwave data** [*interface type number*]

## Syntax Description

<i>interface type number</i>	(Optional) Specifies the interface type and number.
------------------------------	---

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

If the interface is not specified, event data for all interfaces is cleared.

## Examples

The following example shows how to clear Ethernet microwave event data on all interfaces:

```
Device# clear ethernet event microwave data
```



## clear ethernet event microwave statistics

To clear Ethernet microwave event statistics counters for all interfaces or for a specific interface, use the **clear ethernet event microwave statistics** command in privileged EXEC mode.

**clear ethernet event microwave statistics** [*interface type number*]

### Syntax Description

<i>interface type number</i>	(Optional) Specifies the interface type and number.
------------------------------	---

### Command Modes

Privileged EXEC (#)

### Command History

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

### Examples

The following example shows how to clear Ethernet microwave event statistic counters on all interfaces:

```
Device# clear ethernet event microwave statistics
```

# clear ethernet lmi statistics

To clear Ethernet local management interface (LMI) statistics counters for all interfaces or for a specific interface, use the **clear ethernet lmi statistics** command in privileged EXEC mode.

**clear ethernet lmi statistics** [*interface type number*]

## Syntax Description

<b>interface</b>	(Optional) Specifies the interface on which to clear counters.
<i>type</i>	(Optional) String that identifies the type of interface. Valid options are the following: <ul style="list-style-type: none"> <li>• <b>ethernet</b> --Ethernet IEEE 802.3 interface</li> <li>• <b>fastethernet</b> --Fast Ethernet IEEE 802.3 interface</li> <li>• <b>gigabitethernet</b> --Gigabit Ethernet IEEE 802.3z interface</li> </ul>
<i>number</i>	(Optional) Integer that identifies the interface.

## Command Modes

Privileged EXEC (#)

## 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.

## Usage Guidelines

This command resets counters and is useful when you want to monitor Ethernet LMI errors for a period of time. For example, to monitor errors for 1 hour, you would issue the **clear ethernet lmi statistics** command to reset the counter. At the end of the hour, you would issue the **show ethernet lmi statistics** command to display errors that occurred during that one-hour time period.

## Examples

The following example shows how to clear Ethernet LMI statistics counters on all interfaces:

```
Device# clear ethernet lmi statistics
```

Clear "show ethernet lmi" statistics counters on all interfaces [confirm]  
Device#

The following example shows how to clear Ethernet LMI statistics counters on the Gigabit Ethernet 1/0 interface:

Device# **clear ethernet lmi statistics interface gigabitethernet 1/0**  
Clear "show ethernet lmi" statistics counters on this interface [confirm]  
Device#

#### Related Commands

Command	Description
<b>show ethernet lmi</b>	Displays Ethernet LMI Ethernet virtual connections (EVCs) configured on a device.
<b>show interface</b>	Displays statistics for all interfaces configured on a device.

# clear ethernet oam statistics

To reset Ethernet operations, maintenance, and administration (OAM) counters and event statistics on all interfaces or on a specific interface, use the **clear ethernet oam statistics** command in privileged EXEC mode.

**clear ethernet oam statistics** [*interface type number*]

## Syntax Description

<b>interface</b>	(Optional) Specifies an interface.
<i>type</i>	(Optional) Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet.
<i>number</i>	(Optional) Integer from 1 to 9 that is the number of the Ethernet interface.

## 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.

## Usage Guidelines

Use this command when you are debugging or testing and you want all statistics cleared. After this command is issued, the cleared statistics cannot be restored.

## Examples

The following example shows how to clear counters and event statistics for all interfaces:

```
Router# clear ethernet oam statistics
```

## Related Commands

Command	Description
<b>show ethernet oam statistics</b>	Displays detailed information about Ethernet OAM packets.



# clear ethernet ring g8032 statistics

To clear the statistic counters for one or more Ethernet Ring Protocol ( ERP) instances, use the **clear ethernet ring g8032 statistics** command in user EXEC mode.

**clear ethernet ring g8032 statistics** [*ring-name* [**instance** *instance-id*]]

## Syntax Description

<i>ring-name</i>	(Optional) Ethernet ring name.
<b>instance</b> <i>instance-id</i>	(Optional) Enter the <b>instance</b> keyword followed by the instance identifier. The instance identifier is either 1 or 2.

## Command Modes

User EXEC (>)

## 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.

## Usage Guidelines

This command can be used to clear the statistic counters for all ERP instances in an ERP ring, for an ERP instance for a specified ERP ring, or for all ERP instances configured on the device.

## Examples

The following example shows how to enable the **clear ethernet ring g8032 statistics** command.

```
Device> clear ethernet ring g8032 statistics RingA instance 1
```

## clear ethernet service instance

To clear Ethernet service instance attributes such as MAC addresses and statistics or to purge Ethernet service instance errors, use the **clear ethernet service instance** command in privileged EXEC mode.

**clear ethernet service instance** {*id id* *interface type number* {**errdisable**| **mac table** [ *address* ]| **stats**}| *interface type number stats*}

### Syntax Description

<b>id</b>	Indicates that a specific service instance is specified.
<i>id</i>	Identifies the service instance.
<b>interface</b>	Indicates that a specific interface is specified.
<i>type</i>	Type of interface.
<i>number</i>	Number of the interface.
<b>errdisable</b>	Indicates that a clear action for an error-disabled state is specified.
<b>mac table</b>	Indicates that a MAC table is specified.
<i>address</i>	Secure address in the specified MAC table.
<b>stats</b>	Indicates that service instance statistics are specified.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

Use the **clear ethernet service instance** command to clear service instance attributes that are not needed and to purge service instance errors.

## Examples

The following example shows how to clear an error-disabled state on service instance 100 on interface Gigabit Ethernet 1/1:

```
Device(#) clear ethernet service instance id 100 interface GigabitEthernet 1/1 errdisable
```

## Related Commands

Command	Description
show ethernet service instance	Displays information about Ethernet service instances.



# clear lldp

To reset either the Link Layer Discovery Protocol (LLDP) traffic counters or the table that contains LLDP information about neighbors, use the **clear lldp** command in privileged EXEC mode.

**clear lldp {counters| table}**

## Syntax Description

<b>counters</b>	Specifies that the traffic counters are cleared.
<b>table</b>	Specifies that the LLDP table is cleared.

## Command Default

The LLDP traffic counters are not reset, and the table of LLDP information is not cleared.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(33)SXH	This command was introduced.
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 XE Release 3.8S.

## Usage Guidelines

Use this command for informational purposes or to test a symptom of network malfunction such as packet loss.

## Examples

The following example shows how to clear the LLDP counters and display LLDP traffic. The output from the **show lldp traffic** command shows that all the traffic counters have been reset to zero.

```
Device# clear lldp counters
Device# show lldp traffic
LLDP traffic statistics:
  Total frames out: 0
  Total entries aged: 0
  Total frames in: 0
  Total frames received in error: 0
  Total frames discarded: 0
  Total TLVs unrecognized: 0
```

The following example shows how to clear the LLDP table. The output of the **show lldp neighbors** command shows that all information has been deleted from the table.

```
Device# clear lldp table
Device# show lldp neighbors
```

Capability codes:

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device

(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID                      Local Intf                      Hold-time                      Capability                      Port ID

### Related Commands

Command	Description
<b>show lldp</b>	Displays information about LLDP in the network.

## clock destination

To specify the IP address of a Precision Time Protocol clock destination, use the **clockdestination** command in interface configuration mode. To remove a clock destination configuration, use the **no** form of this command.

**clock destination** *clock-ip-address*

**no clock destination** *clock-ip-address*

### Syntax Description

<i>clock-ip-address</i>	IP address of the clock destination.
-------------------------	--------------------------------------

### Command Default

No default behavior or values.

### Command Modes

Clock port configuration (config-ptp-port)

### Command History

Release	Modification
15.0(1)S	This command was introduced.

### Usage Guidelines

If the clock port is set to master mode with unicast and negotiation is disabled, you can only configure a single destination. If the clock port is set to master mode with unicast negotiation, you do not need to use this command because the device uses negotiation to determine the IP address of PTP slave devices.

### Examples

The following example shows how to configure a PTP clock destination:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port masterPort master
Device(config-ptp-port)# clock destination 192.168.1.2
Device(config-ptp-port)# end
```

### Related Commands

Command	Description
<b>clock source</b>	Specifies a PTP clock source.

# clock-port

To specify the clocking mode of a Precision Time Protocol clock port, enter clock port configuration mode using the **clock-port** command in the PTP clock configuration mode. To remove a clocking mode configuration, use the **no** form of this command.

**clock-port** *name* {**slave**|**master**} [**profile g8265.1**]

**no clock-port** *name* {**slave**|**master**}

## Syntax Description

<i>name</i>	Specifies a name for the clock port.
<b>slave</b>	Sets the clock port to PTP slave mode; the port exchanges timing packets with a PTP master device.
<b>master</b>	Sets the clock port to PTP master mode; the port exchanges timing packets with PTP slave devices.
<b>profile g8265.1</b>	(Optional) Sets the clock to use the ITU-T G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling synchronization status message (SSM), and mapping PTP classes.

## Command Default

This command is disabled by default.

## Command Modes

PTP clock configuration (config-ptp-clk)

## Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS Release 3.8S	The <b>profile g8265.1</b> keyword was added on Cisco ASR 901 Series Aggregation Services Routers.

## Usage Guidelines

This command defines a new clock port and enters clock port configuration mode.

Cisco IOS XE Release 3.8S introduces support for telecom profiles, which allow you to configure a clock that uses the ITU-T G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes.

### Examples

The following example shows how to configure a PTP clock port:

```
Device> enable
Device# configure terminal
Device# ptp clock boundary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# clock source 8.8.8.1
Device(config-ptp-port)# sync limit 1
Device(config-ptp-port)# announce timeout 4
Device(config-ptp-port)# delay-req interval 2
Device(config-ptp-port)# end
```

### Related Commands

Command	Description
<b>ptp clock</b>	Creates a PTP clock instance.

## clock source (PTP)

To configure a connection to a Precision Time Protocol (PTP) master device, use the **clock source** command in PTP clock port configuration mode. To remove a clock source configuration, use the **no** form of this command.

**clock source** *source-address*

**no clock source** *source-address*

### Syntax Description

<i>source-address</i>	IP address of the PTP master device.
-----------------------	--------------------------------------

### Command Default

A connection to a PTP master device is not configured.

### Command Modes

PTP clock port configuration (config-ptp-port)

### Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

This command only applies to a clock port in slave mode.

### Examples

The following example shows how to specify a clock source:

```
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# tod 3/0 ntp
Device(config-ptp-clk)# output lpps 3/0
Device(config-ptp-clk)# clock-port slaveport slave
Device(config-ptp-port)# transport ipv4 unicast interface GigabitEthernet3/0/1 negotiation
Device(config-ptp-port)# clock source 103.113.0.1
```

### Related Commands

Command	Description
<b>clock-port</b>	Specifies the mode of a PTP clock port.

## continuity-check

To enable the transmission of continuity check messages (CCMs), use the **continuity-check** command in Ethernet connectivity fault management (CFM) service configuration mode. To disable message transmission, use the **no** form of this command.

**continuity-check** [*interval time*] **loss-threshold** *threshold* [**static rmep**]

**no continuity-check** [*interval time*] **loss-threshold** [**static rmep**]

### Syntax Description

<b>interval</b>	(Optional) Configures the time period between message transmissions.
<i>time</i>	<p>(Optional) Time period between message transmissions. Valid values are as follows:</p> <ul style="list-style-type: none"> <li>• 100ms--100 milliseconds</li> <li>• 10m--10 minutes</li> <li>• 10ms--10 milliseconds</li> <li>• 10s--10 seconds</li> <li>• 1m--1 minute</li> <li>• 1s--1 second</li> <li>• 3.3ms--3.3 milliseconds</li> </ul> <p>The values supported are platform dependent. For the Cisco Catalyst 6500 series switch, the values supported are 10m, 10s, and 1m.</p>
<b>loss-threshold</b>	(Optional) Sets the number of CCMs that should be missed before declaring that a remote maintenance endpoint (MEP) is down.
<i>threshold</i>	(Optional) Integer from 2 to 255. The default is 3.
<b>static</b>	(Optional) Verifies that the MEP received in the CCM is valid.
<b>rmep</b>	(Optional) MEP defined using the <b>mep mpid</b> command.

### Command Default

CCMs are not transmitted.

**Command Modes**

Ethernet CFM service configuration (config-ecfm-srv)

**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.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

**Usage Guidelines**

The static MEP list configured using the **mep mpid** command is used to verify whether a MEP received in a CCM is valid. If the MEP in the received CCM is not configured in the MEP list, an error CCM received fault alarm is set.

Output of the **show running all** command displays “continuity-check interval 1s” when the default interval period is configured and “continuity-check loss-threshold 3” when the default loss threshold is configured.

**Examples**

The following example shows how to configure a loss threshold of 50 CCMs:

```
Device(config)# ethernet cfm domain operatorA level 5
Device(config-ecfm)# service vlan-id 10 port
Device(config-ecfm-srv)# continuity-check loss-threshold 50
```

**Related Commands**

Command	Description
<b>mep mpid</b>	Statically defines MEPs within a maintenance association.
<b>show running all</b>	Shows the running configuration with default values.



## cos (CFM)

To set the class of service (CoS) for a maintenance endpoint (MEP) that will be sent in Ethernet connectivity fault management (CFM) messages, use the **cos** command in the Ethernet CFM interface configuration mode. To set the CoS to the highest priority allowed on the interface, use the **no** form of this command.

**cos** *cos-value*

**no cos**

### Syntax Description

<i>cos-value</i>	Integer from 0 to 7 that identifies the CoS. The default is 0.
------------------	--

### Command Default

If this command is not configured, the default CoS value is used.

### Command Modes

Ethernet CFM interface configuration (config-if-ecfm-mep)

### 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.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

### Usage Guidelines

This command is used to set the priority of messages.

CoS may not be supported on all platforms.

### Examples

The following example shows how to set the CoS to 5:

```
Device(config)# ethernet cfm domain test level 5
Device(config-ecfm)# service vlan-id 17 vlan 17
Device(config-ecfm-srv)# end
Device# configure terminal
Device(config)# interface gigabitethernet 0/2
Device(config-if)# ethernet cfm mep domain test mpid 5 vlan 17
Device(config-if-ecfm-mep)# cos 5
```

# delay-req interval

To specify a recommended interval for Precision Time Protocol member devices to send delay request messages, use the **delay-req interval** command in PTP clock port configuration mode. To remove a delay request interval configuration, use the **no** form of this command.

**delay-req interval** *interval-value* **unicast**  
**no delay-req interval** *interval-value* **unicast**

## Syntax Description

<i>interval-value</i>	<p>Specifies the length of the interval for delay request messages. The intervals are set using log base 2 values, as follows:</p> <ul style="list-style-type: none"> <li>• 4--1 packet every 16 seconds</li> <li>• 3--1 packet every 8 seconds</li> <li>• 2--1 packet every 4 seconds</li> <li>• 1--1 packet every 2 seconds</li> <li>• 0--1 packet every second</li> <li>• -1--1 packet every 1/2 second, or 2 packets per second</li> <li>• -2--1 packet every 1/4 second, or 4 packets per second</li> <li>• -3--1 packet every 1/8 second, or 8 packets per second</li> <li>• -4--1 packet every 1/16 seconds, or 16 packets per second.</li> <li>• -5--1 packet every 1/32 seconds, or 32 packets per second.</li> <li>• -6--1 packet every 1/64 seconds, or 64 packets per second.</li> </ul> <p>The recommended value is -6.</p>
<b>unicast</b>	(Optional) Specifies that the device send PTP delay request messages using unicast mode.

**Command Default** The default value is -4 (16 packets per second).

**Command Modes** PTP clock-port configuration (config-ptp-port)

**Command History**

Release	Modification
15.0(1)S	This command was introduced.

**Usage Guidelines**

This configuration is only required when an interface is in PTP slave mode.

**Examples**

The following example shows how to use the **delay-req** command:

```
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# clock-port slaveport slave
Router(config-ptp-port)# delay-req interval 2 unicast
Router(config-ptp-port)# end
Router#
```

**Related Commands**

Command	Description
<b>clock-port</b>	Specifies the mode of a PTP clock port.

## description (Ethernet ring)

To specify a descriptive name for an Ethernet ring instance, use the **description** command in Ethernet ring instance configuration mode. To remove the descriptive name, use the **no** form of this command.

**description** *descriptive-name*

**no description**

### Syntax Description

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

### Command Default

A descriptive name is not given to the Ethernet ring instance.

### 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.

### Examples

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

```
Device> enable
Device# configure terminal
Device(config)# ethernet ring g8032 r1
Device(config-erp-ring)# instance 1
Device(config-erp-inst)# description cisco_customer_instance
```

# description (mac-tunnel)

To describe the name and purpose of a MAC tunnel or a service instance under a MAC tunnel, use the **description** command in either MAC-in-MAC tunnel configuration mode or MAC tunnel service configuration mode. To remove a description, use the **no** form of this command.

**description** *description*

**no description** *description*

## Syntax Description

<i>description</i>	String of a maximum of 240 characters. <ul style="list-style-type: none"> <li>• In MAC-in-MAC tunnel configuration mode, the description is of the MAC tunnel.</li> <li>• In MAC tunnel service configuration mode, the description is of the service instance.</li> </ul>
--------------------	--

## Command Default

MAC tunnels or a service instances under MAC tunnels do not have descriptions.

## Command Modes

MAC-in-MAC tunnel configuration (config-tunnel-minm) MAC tunnel service configuration (config-tunnel-srv)

## Command History

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

## Usage Guidelines

Use this command to identify and describe the type of service for which the MAC tunnel is used.

## Examples

The following example shows how to add descriptions for both a MAC tunnel and a service instance under that MAC tunnel:

```
Router(config)# ethernet mac-tunnel virtual 100
Router(config-tunnel-minm)# description MAC-Tunnel-100
Router(config-tunnel-minm)# service instance 1 ethernet
Router(config-tunnel-srv)# description ServInst-1
```

## disable (CFM-AIS-link)

To disable the generation of Alarm Indication Signal (AIS) frames resulting from a link-status change (server maintenance endpoint [SMEP]), use the **disable** command in CFM SMEP AIS configuration mode (config-ais-link-cfm). To enable AIS frame generation, use the **no** form of this command.

**disable**

**no disable**

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

**Command Default** AIS frames are generated.

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

Command History	Release	Modification
	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** When the default value is configured, “no disable” is displayed when the **show running all** command is issued.

**Examples** The following example shows how to disable AIS frame generation after a link-status change:

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

### Related Commands

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

## encapsulation dot1ah isid

To configure dot1ah encapsulation for a specific service instance ID (I-SID), use the **encapsulation dot1ah isid** command in MAC tunnel service configuration mode. To remove dot1ah encapsulation for an I-SID, use the **no** form of this command.

**encapsulation dot1ah isid** *isid*

**no encapsulation dot1ah isid** *isid*

### Syntax Description

<i>isid</i>	Integer from 1 to 16777215 that identifies the I-SID.
-------------	---

### Command Default

Encapsulation is not configured.

### Command Modes

MAC tunnel service configuration (config-tunnel-srv)

### Command History

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

### Usage Guidelines

The I-SID is used to indicate a service in the provider backbone bridge (PBB) network. You can define the service, which can be a customer or a particular customer and type of data; for example, voice or video.

### Examples

The following example shows how to configure dot1ah encapsulation for I-SID 500:

```
Router(config)# ethernet mac-tunnel virtual 1
Router(config-tunnel-mimn)# service instance 1 ethernet
Router(config-tunnel-srv)# encapsulation dot1ah isid 500
```

## errdisable recovery cause mac-security

To enable automatic recovery of a service instance after a MAC security violation, use the **errdisable recovery cause mac-security** command in service instance configuration mode. To disable the automatic recovery mechanism, use the **no** form of this command.

**errdisable recovery cause mac-security** *interval*

**no errdisable recovery cause mac-security** *interval*

### Syntax Description

<i>interval</i>	Time, in seconds, to recover from a MAC security violation. Range is 30 to 86400.
-----------------	---

### Command Default

Automatic recovery of a service instance is disabled.

### Command Modes

Service instance configuration (config-if-srv)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S

### Usage Guidelines

A cause is the reason why the error-disabled state occurred. When a cause is detected on a service instance, the service instance is placed in the error-disabled state (an operational state that is similar to the shutdown state). When you enable automatic error recovery, the service instance is brought out of the error-disabled state and allowed to retry the operation after all the causes have timed out. If you do not enable automatic error recovery, the service instance stays in the error-disabled state until the **shutdown** and **no shutdown** commands are issued.

Alternatively, you can use the **clear ethernet service instance** command to bring the service instance out of the error-disabled state.

### Examples

The following example shows how to enable the automatic recovery of service instance 200 after a MAC security violation and to specify a recovery time of 30 seconds.

```
Device>
enable
Device#
configure terminal
Device(config)# interface gigabitethernet 3/0/1
Device(config-if)# service instance 200 ethernet
Device(config-if-srv)# encapsulation dot1q 200
```



```
Device(config-if-srv) # bridge-domain 100
Device(config-if-srv) # mac security
Device(config-if-srv) # errdisable recovery cause mac-security 30
```

**Related Commands**

Command	Description
<b>clear ethernet service instance</b>	Clears the Ethernet service instance error-disable state.
<b>show ethernet service instance</b>	Displays information about Ethernet service instances.

# errdisable recovery cause mlacp-minlink

To enable automatic recovery from a failover state of the port channel, use the **errdisable recovery cause mlacp-minlink** command in global configuration mode. To disable this command, use the **no** form of this command.

**errdisable recovery cause mlacp-minlink**

**[no] errdisable recovery cause mlacp-minlink**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is disabled by default. If the **errdisable recovery cause mlacp-minlink** is not enabled, the links stay in the ERR\_DISABLE state until a shut/no shut is entered on the links.

## Command Modes

Global config (config#)

## Command History

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

## Usage Guidelines

Use the **errdisable recovery cause mlacp-minlink** command to enable automatic recovery on the interface from the ERR\_DISABLE state. This command tries to bring the port-channel interface out of the ERR\_DISABLE state and retry operation after all the causes have timed out. To set the interval for recovery, configure the **errdisable recovery interval** *seconds* command.

## Examples

The following example shows how to enable recovery from the ERR\_DISABLE state and set the interval to 100 seconds:

```
errdisable recovery cause mlacp-minlink
errdisable recovery interval 100
```

## Related Commands

Command	Description
<b>lacp failover</b>	Sets the mLACP switchover to non-revertive or brute force.
<b>errdisable recovery interval</b>	Sets the interval time for recovery from the ERR_DISABLE state.

## ethernet cfm ais

To configure Ethernet Connectivity Fault Management (CFM) Alarm Indication Signal (AIS) generation from a server maintenance endpoint (SMEP), use the **ethernet cfm ais** command in global configuration mode. To disable AIS generation from an SMEP, use the **no** form of this command.

**ethernet cfm ais** {**domain** *domain-name*| {**evc name**| **vlan** *vlanid*| {*vlanid-vlanid*| , *vlanid-vlanid*}} **link-status** **global**}}

**no ethernet cfm ais** {**domain** *domain-name*| {**evc name**| **vlan** *vlanid*| {*vlanid-vlanid*| , *vlanid-vlanid*}} **link-status** **global**}}

### Syntax Description

<b>domain</b> <i>domain-name</i>	Indicates that a maintenance domain is specified. Specify a string of a maximum of 154 characters that identifies the domain.
<b>evc</b> <i>name</i>	Indicates that an Ethernet virtual circuit (EVC) is specified. Specify a string identifying the EVC name.
<b>vlan</b> <i>vlanid</i>	Indicates that a VLAN is specified. Integer in the range from 1 to 4094 identifying the VLAN. Integers in the range from 1 to 4094, separated by commas, that list VLANs to be enabled.
<i>vlanid</i> - <i>vlanid</i>	Integers in the range from 1 to 4094 that define a range of VLANs to be enabled. The hyphen is required to separate the starting and ending values that define the range.
, <i>vlanid</i> - <i>vlanid</i>	Integers in the range from 1 to 4094 that define a list of VLAN ranges to be enabled. 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 to be enabled.
<b>link-status</b>	Enables or disables AIS generation from an SMEP on an interface supporting 802.3ah interworking.
<b>global</b>	Places the CLI in Ethernet CFM AIS MEP configuration mode to configure AIS-specific commands for an SMEP with 802.3ah interworking.

**Command Default** AIS generation is enabled.

**Command Modes** Global configuration (config)

## Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS 12.2(50)SY release.

## Usage Guidelines

The **ethernet cfm ais** command allows you to configure, enable, or disable AIS generation from an MEP or SMEP. To change the default values for AIS generation on an SMEP, use the **link-status global** keywords. To change the default values for AIS generation on an MEP, use the **domain** keyword.

## Examples

The following example shows how to specify AIS generation on a domain named PROVIDER and on VLAN 10:

```
Router(config)# ethernet cfm ais domain PROVIDER vlan 10
```

The following example shows how to enable AIS generation and place the CLI in Ethernet CFM AIS MEP configuration mode:

```
Router(config)# ethernet cfm ais link-status global
Router(config-ais-mep-cfm)#
```

## Related Commands

Command	Description
<b>clear ethernet cfm ais</b>	Clears an MEP or SMEP of the AIS defect condition.

## ethernet cfm ais link-status

To enable Alarm Indication Signal (AIS) generation from a server maintenance endpoint (SMEP), use the **ethernet cfm ais link-status** command in interface configuration mode. To disable AIS generation, use the **no** form of this command.

**ethernet cfm ais link-status** [*level level-id*] *period seconds*

**no ethernet cfm ais link-status** [*level*] *period*

### Syntax Description

<b>level</b>	(Optional) Indicates a maintenance domain level where the AIS will be sent.
<i>level-id</i>	(Optional) Integer from 0 to 7 that identifies the maintenance level.
<b>period</b>	(Optional) Configures the AIS transmission period generated by the SMEP on the interface.
<i>seconds</i>	(Optional) Integer value 1 or 60 that indicates the AIS transmission period in seconds. The default is 60.

### Command Default

AIS frames are not generated.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
15.0(1)XA	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
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 has precedence over the **ethernet cfm ais link-status global** command issued in global configuration mode.

## Examples

The following example shows how to configure AIS generation with a transmission period of 60 seconds:

```
Device(config-if)# ethernet cfm ais link-status period 60
Device(config-if)#
```

## Related Commands

Command	Description
<b>ethernet cfm ais link-status global</b>	Globally enables AIS generation and places the CLI in CFM SMEP AIS configuration mode.

## ethernet cfm ais link-status global

To globally enable Alarm Indication Signal (AIS) generation and place the CLI in Ethernet Connectivity Fault Management (CFM) AIS MEP configuration mode, use the **ethernet cfm ais link-status global** command in global configuration mode. To remove the global AIS configuration, use the **no** form of this command.

**ethernet cfm ais link-status global**

**no ethernet cfm ais link-status global**

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

**Command Default** AIS generation is enabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(33)SRD	This command was introduced.
	15.0(1)XA	This command was integrated into Cisco IOS Release 15.0(1)XA.
	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.

**Usage Guidelines** The **ethernet cfm ais link-status global** command changes configuration modes to allow you to configure AIS commands for an SMEP.

**Examples** The following example shows how to configure AIS commands for an SMEP:

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

# ethernet cfm alarm

To configure an alarm for Ethernet connectivity fault management (CFM), use the **ethernet cfm alarm** command in global configuration mode. To restore the command options' default values, use the **no** form of this command.

**ethernet cfm alarm** {*delay milliseconds*| **notification** {**all**| **error-xcon**| **mac-remote-error-xcon**| **none**| **remote-error-xcon**| **xcon**}} [**packet** *max-num*| **reset milliseconds**]

**no ethernet cfm alarm** {*delay*| **notification** {**all**| **error-xcon**| **mac-remote-error-xcon**| **none**| **remote-error-xcon**| **xcon**}} [**packet**| **reset**]

## Syntax Description

<b>delay</b>	Sets a delay time value during which one or more defects must be present before a fault alarm is issued.
<i>milliseconds</i>	Integer from 2500 to 10000 that specifies the number of milliseconds (ms) for either a delay or a reset of an alarm.  • The default is 2500 for the <b>delay</b> option. The default is 10000 for the <b>reset</b> option.
<b>notification</b>	Sets the defects that are to be reported if fault alarms are enabled. This configuration is global and can be overridden by the fault alarm configurations on a supported interface.
<b>all</b>	Reports all defects: DefRDI, DefMACStatus, DefRemote, DefError, and DefXcon.
<b>error-xcon</b>	Reports only DefError and DefXcon defects.
<b>mac-remote-error-xcon</b>	Reports only DefMACStatus, DefRemote, DefError, and DefXcon (default) defects. This option is the default.
<b>none</b>	No defects are reported.
<b>remote-error-xcon</b>	Reports only DefRemote, DefError, and DefXcon defects.
<b>xcon</b>	Reports only DefXcon defects.
<b>packet</b>	Reports DefError and DefXcon fault alarm packets.
<i>max-num</i>	Integer from 1 to 65535 that specifies the maximum number of DefError and DefXcon packets. The default is 0.



<b>reset</b>	Sets a reset time value during which, after a fault alarm, no defects must be present before another fault alarm is enabled.
--------------	--

**Command Default** Ethernet CFM alarms are disabled.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SX12	This command was introduced.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
	12.2(54)SE	This command was modified. Support for the <b>packet</b> keyword and <i>max-num</i> argument was added.
	15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
	Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

**Usage Guidelines** If a higher priority defect occurs after a lower priority defect has triggered an alarm but before the alarm has reset, immediately issue another fault alarm for the higher priority defect.

Output of the **show running all** command displays “ethernet cfm alarm delay 2500” when the default value for the delay option is configured and “ethernet cfm alarm reset 10000” when the default value for the reset option is configured.

**Examples** The following example shows how to set up notification for all defects:

```
Device(config)# ethernet cfm alarm notification all
The following example shows how to set the time during which one or more defects must be
present before a fault alarm is issued to 5000 ms:
Device(config)# ethernet cfm alarm delay 5000
The following example shows how to set the maximum number of DefError and DefXcon fault
alarm packets to 6500:
Device(config)# ethernet cfm alarm packet 6500
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show running all</b>	Displays the running configuration with default values.

# ethernet cfm cc

To set the parameters for continuity check messages (CCMs), use the **ethernet cfm cc** command in global configuration mode. To reset parameters to their default values, use the **no** form of this command.

**ethernet cfm cc level** {**any**| *level-id*| *level-id -level-id*| ,*level-id-level-id*} {**evc** *evc-name*| **vlan** {*vlan-id*| **any**| *vlan-id-vlan-id*| ,*vlan-id-vlan-id*}} [**interval** *seconds*] [**loss threshold** *num-msgs*]

**no ethernet cfm cc level** {**any**| *level-id*| *level-id -level-id*| ,*level-id-level-id*} {**evc** *evc-name*| **vlan** {*vlan-id*| **any**| *vlan-id-vlan-id*| ,*vlan-id-vlan-id*}} [**interval** *seconds*] [**loss threshold** *num-msgs*]

## Syntax Description

<b>level</b>	Indicates a maintenance level for the configuration.
<b>any</b>	Indicates that all levels are to be configured.
<i>level-id</i>	Integer from 0 to 7 that identifies a maintenance level.
<i>level-id -level-id</i>	Integers from 0 to 7 that define a range of levels to be configured. The hyphen is required to separate starting and ending values that define the range.
, <i>level-id - level-id</i>	(Optional) Integers from 0 to 7 that define a list of 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 levels to be configured.
<b>evc</b>	Indicates an Ethernet virtual circuit (EVC) is configured.
<i>evc-name</i>	String that identifies the EVC.
<b>vlan</b>	Indicates a VLAN for configuration.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies a VLAN to be configured.
<b>any</b>	Indicates that all VLANs are 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>	(Optional) 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.
<b>interval</b>	(Optional) Specifies, in seconds, the time between CCM transmissions.
<i>seconds</i>	(Optional) Integer value in the range of 10 to 65535. The default is 30.
<b>loss-threshold</b>	(Optional) Indicates the maximum number of CCMs that can be missed before declaring that a maintenance endpoint (MEP) is down.
<i>num-msgs</i>	(Optional) Integer in the range of 2 to 255 that specifies the maximum number of CCMs that can be lost before a MEP is declared down. The default is 2.

**Command Default**

For all maintenance levels and VLANs configured on a device, the interval is 30 seconds and the loss-threshold is 2.

**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)SRD	This command was modified. 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.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
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

The **ethernet cfm cc** command is used to set parameters for generating and receiving CCMs in one of the following ways:

- Globally (per device)
- For a maintenance domain
- For a particular customer service instance (CSI)
- For a combination of maintenance domain and CSI

When the **ethernet cfm cc** command is issued, the system may perform optimizations by concatenating possible ranges, and the configuration may not go through nonvolatile generation (NVGEN) as it was originally entered.

If you configure the **ethernet cfm cc** command with the default values for interval and loss threshold, these parameters will not display after NVGEN. If you configure the command with at least one parameter not at the default value, all parameters are displayed.

An EVC is an association of two or more user network interfaces (UNIs).



### Note

This command is not supported in the Connectivity Fault Management 802.1ag Standard (CFM IEEE).

## Examples

The following example shows how to configure an Ethernet CFM level ID of 5 for all VLANs, with messages transmitted every 30 seconds and a remote MEP declared down after two messages are missed. Note that the interval and loss-threshold parameters are configured for the default values and do not display after NVGEN.

```
Device(config)# ethernet cfm cc level 5 vlan any interval 30 loss-threshold 2
(NVGEN)ethernet cfm cc level 5 vlan any
```

The following example shows how to configure an Ethernet CFM level ID of 5 for all VLANs, with messages transmitted every 1000 seconds and a remote MEP declared down after two messages (the default value) are missed:

```
Device(config)# ethernet cfm cc level 5 vlan any interval 1000 loss-threshold 2
(NVGEN)ethernet cfm cc level 5 vlan any interval 1000
```

The following example shows how to configure an Ethernet CFM level ID of 5 for all VLANs, with messages transmitted every 1000 seconds and a remote MEP declared down after 7 messages are missed (neither value is a default value):

```
Device(config)# ethernet cfm cc level 5 vlan any interval 1000 loss-threshold 7
(NVGEN)ethernet cfm cc level 5 vlan any interval 1000 loss-threshold 7
```

The following example shows how to configure Ethernet CFM for multiple levels for VLANs 100 to 200 with messages transmitted every 50 seconds and a remote MEP declared down after 5 messages are missed (neither value is a default value):

```
Device(config)# ethernet cfm cc level 1-5 vlan 100-200 interval 50 loss-threshold 5

Device(config)# no ethernet cfm cc level 2-3 vlan 50-150 interval 50 loss-threshold 5
(
NVGEN)ethernet cfm cc level 2-3 vlan 151-200 interval 50 loss-threshold 5
      ethernet cfm cc level 1,4-5 vlan 100-200 interval 50 loss-threshold 5
```

The following example shows how to configure Ethernet CFM level ID of 5 for EVC evc5, with messages transmitted every 50 seconds and a remote MEP declared down after 3 messages are missed (neither value is a default value):

```
Device(config)# ethernet cfm cc level 5 evc evc5 interval 50 loss-threshold 3
(
NVGEN)ethernet cfm cc level 5 evc evc5 interval 50 loss-threshold 3
```

## ethernet cfm cc enable level evc

To globally enable transmission of continuity check messages (CCMs), use the **ethernet cfm cc enable level evc** command in global configuration mode. To disable transmission of CCMs, use the **no** form of this command.

**ethernet cfm cc enable level** {**any**| *level-id*| , *level-id*| *level-id* -*level-id*| , *level-id*-*level-id*}**evc** *evc-name*

**no ethernet cfm cc enable level** {**any**| *level-id*| , *level-id*| *level-id*-*level-id*| , *level-id*-*level-id*}**evc** *evc-name*

<b>any</b>	Enables CCMs for all levels.
<i>level-id</i>	Integer from 0 to 7 that identifies a maintenance level.
, <i>level-id</i>	Integers from 0 to 7, separated by commas, that list levels to be enabled.
<i>level-id</i> - <i>level-id</i>	Integers from 0 to 7 that define a range of levels to be enabled. The hyphen is required to separate starting and ending values that define the range.
, <i>level-id</i> - <i>level-id</i>	Integers from 0 to 7 that define a list of ranges to be enabled. 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 levels to be enabled.
<i>evc-name</i>	String that identifies the Ethernet virtual circuit (EVC).

### Command Default

No CCMs are transmitted.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

Use the **ethernet cfm cc enable level evc** command to enable transmission of CCMs in one of the following ways:

- Globally (per device)

- For a particular level
- For a particular EVC
- For a combination of level and EVC

## Examples

The following example shows how to configure the **ethernet cfm cc enable level evc** command for EVC evc5:

```
Router (config)# ethernet cfm cc enable level 5 evc evc5
```

How you enter the **ethernet cfm cc enable level evc** command and the format you see in the configuration may be different. For example, if you enter:

```
Router(config)# ethernet cfm cc enable level 1,2,3,4,5 evc evc1
```

The configuration shows the following:

```
ethernet cfm cc enable level 1-5 evc evc1
```

To shorten the length of the command, you also can enter it as shown in the following example:

```
Router(config)# ethernet cfm cc enable level 1-5 evc evc1
```

## Related Commands

Command	Description
<b>ethernet cfm cc enable level vlan</b>	Enables transmission of CCMs.

## ethernet cfm cc enable level vlan

To globally enable transmission of continuity check messages (CCMs), use the **ethernet cfm cc enable level vlan** command in global configuration mode. To disable transmission of CCMs, use the **no** form of this command.

**ethernet cfm cc enable level** {**any**| *level-id* | *level-id level-id-level-id* | *level-id-level-id*} **vlan** {**any**| *vlan-id* | *vlan-id vlan-id-vlan-id* | *vlan-id-vlan-id*}

**no ethernet cfm cc enable level** {**any**| *level-id* | *level-id level-id-level-id* | *level-id-level-id*} **vlan** {**any**| *vlan-id* | *vlan-id vlan-id-vlan-id* | *vlan-id-vlan-id*}

### Syntax Description

<b>any</b>	Enables CCMs for all levels.
<i>level-id</i>	Integer from 0 to 7 that identifies a maintenance level.
, <i>level-id</i>	Integers from 0 to 7, separated by commas, that list levels to be enabled.
<i>level-id - level-id</i>	Integers from 0 to 7 that define a range of levels to be enabled. The hyphen is required to separate starting and ending values that define the range.
, <i>level-id - level-id</i>	Integers from 0 to 7 that define a list of ranges to be enabled. 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 levels to be enabled.
<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 CCMs are transmitted.

**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.
	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** Use the **ethernet cfm cc enable level vlan** command to enable transmission of CCMs in one of the following ways:

- Globally (per device)
- For a particular level
- For a particular VLAN
- For a combination of level and VLAN

How you enter the **ethernet cfm cc enable level vlan** command and the format you see in the configuration may be different. For example, if you enter:

```
Device(config)# ethernet cfm cc enable level 1,2,3,4,5 vlan 100,101,102,103,105
```

The configuration shows the following:

```
ethernet cfm cc enable level 1-5 vlan 100-103,105
```

To shorten the length of the command, you also can enter it this way.

**Examples** The following examples show how this command functions:

- 1 The command already configured is:

```
ethernet cfm cc enable level 1-5 vlan 100-200
```

- 2 You configure this new command:

```
Device(config)# no
ethernet cfm cc enable level 2-3 vlan 50-150
```

- 3 The following commands are generated as a result of the command you have just configured. Note that these commands are different from the command you entered.

```
ethernet cfm cc enable level 1,4-5 vlan 100-200  
ethernet cfm cc enable level 2-3 vlan 151-200
```

# ethernet cfm distribution enable

To enable Ethernet connectivity fault management (CFM) distribution, use the **ethernetcfmdistributionenable** command in the global configuration mode. To disable distribution, use the **no** form of this command.

**ethernet cfm distribution enable**

**no ethernet cfm distribution enable**

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

**Command Default** Ethernet CFM distribution is disabled when this command is not configured.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	15.1(2)S	This command was introduced.
	Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

**Usage Guidelines** On the Cisco 7600 series router, this command must be configured before Ethernet performance monitoring (EPM) sessions are configured.

When you issue the **noethernetcfmdistributionenable** command, all EPM sessions on the route processor and on the line card are removed, but the IP SLA configurations remain. If you do not want any Y.1731 performance monitoring sessions, you must remove the IP SLA configurations. You can use the **ipslareset** command to clear all the IP SLA configurations, or you can clear each one individually.

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

```
Device(config)# ethernet cfm distribution enable
```

# ethernet cfm domain level

To define a connectivity fault management (CFM) maintenance domain at a particular maintenance level and enter Ethernet CFM configuration mode, use the **ethernet cfm domain level** command in global configuration mode. To remove the CFM domain at the specified level, use the **no** form of this command.

**ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**]

**no ethernet cfm domain** *domain-name* **level** *level-id*

## Syntax Description

<i>domain-name</i>	String of a maximum of 154 characters that identifies the domain.
<i>level-id</i>	Integer from 0 to 7 that identifies the maintenance level.
<b>direction outward</b>	(Optional) Specifies the domain direction as outward (toward the wire). The default direction is inward.  <b>Note</b> Support for the <b>outward</b> keyword varies by Cisco release.

## Command Default

No maintenance domains are assigned to maintenance levels if this command is not issued.

## 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. The <b>direction outward</b> keywords were added.
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.
Cisco IOS XE Release 3.7S	This command was modified. Support for short maintenance-association (MA) names was added.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

## Usage Guidelines

When a device is in Ethernet CFM configuration mode, parameters specific to a maintenance domain can be set. Several domains, with different names, can be configured at the same maintenance level; however, a single domain cannot be associated with multiple levels.

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.

When this command places the CLI in Ethernet configuration mode, in CFM D1 the mode prompt is "config-ether-cfm" and in CFM IEEE the mode prompt is "config-ecfm."

When you configure PORT/DOWN services on platforms that support multiple MAs per domain (that is, platforms that have a multiple capability bit set), entering a new short MA name for the service creates a new MA.

## Examples

The following example shows how to define an outward facing domain named domain1 at level 6 and that the CLI mode changes to Ethernet CFM configuration mode:

```
Device(config)# ethernet cfm domain domain1 level 6 direction outward
Device(config-ether-cfm)#
```

The following example shows how to define a domain named cust10 at level 5 and also shows the Ethernet CFM configuration mode prompt that is displayed in the CFM IEEE Standard implementation:

```
Device(config)# ethernet cfm domain cust10 level 5
Device(config-ecfm)#
```

## Related Commands

Command	Description
<b>show ethernet cfm domain</b>	Displays information about maintenance points configured on a device.
<b>show ethernet cfm maintenance-points local</b>	Displays information about maintenance points configured on a device.

# ethernet cfm enable (interface)

To enable connectivity fault management (CFM) processing on an interface, use the **ethernet cfm enable** command in interface configuration mode. To disable CFM processing on an interface, use the **no** form of this command.

**ethernet cfm enable**

**no ethernet cfm enable**

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

**Command Default** Ethernet CFM is enabled.

**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.
	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** Ethernet CFM is enabled by default on an interface and must be disabled explicitly. When CFM is disabled on an interface, hardware resources (for example, port-ASIC match-registers) are released for that interface. This command is mutually exclusive of maintenance intermediate point (MIP) and maintenance endpoint (MEP) configuration commands. The interface must be enabled before any MEPs or MIPs can be configured. Similarly, disabling a port that has MIPs or MEPs configured is not allowed. The user must first unconfigure the maintenance points.

When CFM processing is disabled on an interface, all CFM frames that arrive at that interface are forwarded as normal data traffic, and are not processed by the CPU.

**Examples** The following example shows how to disable and then enable CFM processing on an interface:

```
Device(config-if) # no ethernet cfm enable
Device(config-if) # ethernet cfm enable
```

# ethernet cfm enable

**Note**

Effective with Cisco IOS XE Release 3.6S, the **ethernet cfm enable** command is not available in Cisco IOS software.

To enable connectivity fault management (CFM) processing globally on a device, use the **ethernet cfm enable** command in global configuration mode. To disable CFM processing globally on a device, use the **no** form of this command.

**ethernet cfm enable**

**no ethernet cfm enable**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Ethernet CFM 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.
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 XE Release 3.6S	This command was removed.

**Usage Guidelines**

Ethernet CFM is disabled by default and must be enabled explicitly. When CFM is configured, hardware resources (for example, port-ASIC match-registers) are allocated for CFM.

**Examples**

The following example shows how to enable CFM processing globally on a device:

```
Device(config)# ethernet cfm enable
```

# ethernet cfm global

To enable Ethernet connectivity fault management (CFM) globally on a device, use the **ethernet cfm global** command in global configuration mode. To disable CFM globally on a device, use the **no** form of this command.

**ethernet cfm global**

**no ethernet cfm global**

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

**Command Default** Ethernet CFM is disabled.

**Command Modes** Global configuration (config)

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** Ethernet CFM is disabled by default and must be enabled explicitly. When CFM is configured, hardware resources (for example, port-ASIC match registers) are allocated for CFM.

This command is supported only in the Ethernet CFM IEEE 802.1ag Standard implementation.

**Examples** The following example shows how to enable CFM globally on a device:

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



## ethernet cfm ieee

To enable the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM, use the **ethernet cfm ieee** command in global configuration mode. To disable the CFM IEEE version, use the **no** form of this command.

**ethernet cfm ieee**

**no ethernet cfm ieee**

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

**Command Default** Ethernet CFM IEEE is disabled.

**Command Modes** Global configuration (config)

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** This command is auto-generated when CFM is enabled and running IEEE CFM. In Cisco pre-Standard CFM Draft 1 (CFM D1), this command is not supported.

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

```
Device(config)# ethernet cfm ieee
```

# ethernet cfm interface

To enable Ethernet connectivity fault management (CFM) processing on a port, use the **ethernet cfm interface** command in interface configuration mode. To disable Ethernet CFM processing, use the **no** form of this command.

**ethernet cfm interface**

**no ethernet cfm interface**

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

**Command Default** CFM processing is enabled.

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

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** This command is mutually exclusive of the maintenance intermediate point (MIP) and maintenance endpoint (MEP) configuration commands. A port must be enabled before any MEPs or MIPs can be configured. Similarly, maintenance points must be unconfigured before a port configured with MIPs or MEPs can be disabled.

When CFM processing is disabled on a port, all CFM frames that arrive at that port are dropped and are not processed by the CPU.

CFM is enabled by default on a port and must be disabled explicitly. When CFM is disabled on a port, hardware resources such as port-ASIC match registers are released for that port.

**Examples** The following example shows how to configure an Ethernet interface for CFM processing:

```
Device(config-if)# ethernet cfm interface
Device(config-if)#
```

# ethernet cfm logging

To enable Ethernet Connectivity Fault Management (CFM) syslog messages, use the **ethernet cfm logging** command in global configuration mode. To disable CFM syslog messages, use the **no** form of this command.

## Cisco pre-Standard CFM Draft 1 (CFM D1)

**ethernet cfm logging** [ais| alarm {cisco| ieee}]

**no ethernet cfm logging** [ais| alarm {cisco| ieee}]

## CFM IEEE 802.1ag Standard (CFM IEEE)

**ethernet cfm logging** [ais| alarm {cisco| ieee}| lck]

**no ethernet cfm logging** [ais| alarm {cisco| ieee}| lck]

### Syntax Description

<b>ais</b>	(Optional) Enables syslog messages specific to the CFM Alarm Indication Signal (AIS) feature.
<b>alarm</b>	(Optional) Specifies an alarm.
<b>cisco</b>	(Optional) Enables alarm syslog messages for Cisco MIBs.
<b>ieee</b>	(Optional) Enables alarm syslog messages for IEEE MIBs for all VLAN services.
<b>lck</b>	(Optional) Enables syslog messages specific to the CFM Locked Signal function (LCK).

### Command Default

CFM logging is not enabled.

### Command Modes

Global configuration (config)

### Command History

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

## Examples

The following example shows how to enable all Ethernet CFM syslog messages:

```
Device(config)# ethernet cfm logging
```

The following example shows how to enable all alarm syslog messages for Cisco MIBs:

```
Device(config)# ethernet cfm logging alarm cisco
```

The following example shows how to enable syslog messages specific to the CFM AIS feature:

```
Device(config)# ethernet cfm logging ais
```



## ethernet cfm mep crosscheck through location prefer

---

- [ethernet cfm mep crosscheck, page 102](#)
- [ethernet cfm mep crosscheck start-delay, page 105](#)
- [ethernet cfm mep domain mpid, page 107](#)
- [ethernet cfm mep level mpid vlan, page 109](#)
- [ethernet cfm mip, page 113](#)
- [ethernet cfm mip level, page 115](#)
- [ethernet cfm slm max, page 117](#)
- [ethernet cfm slm timeout, page 119](#)
- [ethernet cfm traceroute cache, page 121](#)
- [ethernet cfm traceroute cache hold-time, page 123](#)
- [ethernet cfm traceroute cache size, page 125](#)
- [ethernet event microwave, page 127](#)
- [ethernet evc, page 129](#)
- [ethernet lmi, page 131](#)
- [ethernet lmi ce-vlan map, page 133](#)
- [ethernet lmi global, page 135](#)
- [ethernet lmi interface, page 137](#)
- [ethernet loopback local interface, page 139](#)
- [ethernet loopback permit, page 141](#)
- [ethernet mac-flush notification mirp, page 143](#)
- [ethernet mac limit action flooding disable, page 145](#)
- [ethernet mac limit maximum addresses, page 147](#)
- [ethernet mac-tunnel virtual, page 148](#)

- [ethernet oam, page 149](#)
- [ethernet oam link-monitor frame, page 152](#)
- [ethernet oam link-monitor frame-period, page 154](#)
- [ethernet oam link-monitor frame-seconds, page 156](#)
- [ethernet oam link-monitor high-threshold action, page 158](#)
- [ethernet oam link-monitor on, page 160](#)
- [ethernet oam link-monitor receive-crc, page 162](#)
- [ethernet oam link-monitor supported, page 164](#)
- [ethernet oam link-monitor symbol-period, page 166](#)
- [ethernet oam link-monitor transmit-crc, page 168](#)
- [ethernet oam mib log size, page 170](#)
- [ethernet oam remote-loopback, page 171](#)
- [ethernet oam remote-loopback \(interface\), page 173](#)
- [ethernet ring g8032, page 175](#)
- [ethernet ring g8032 profile, page 176](#)
- [ethernet subscriber, page 177](#)
- [ethernet subscriber session, page 179](#)
- [ethernet subscriber static, page 181](#)
- [ethernet tcn-propagation, page 183](#)
- [ethernet uni, page 184](#)
- [event ethernet microwave clear-sd, page 186](#)
- [event ethernet microwave sd, page 188](#)
- [exclusion-list, page 190](#)
- [id \(CFM\), page 192](#)
- [inclusion-list, page 193](#)
- [initiator unclassified vlan, page 195](#)
- [input, page 197](#)
- [instance \(Ethernet ring\), page 199](#)
- [l2 subscriber, page 200](#)
- [lacp active-port distribution automatic, page 202](#)
- [lacp direct-loadswap, page 204](#)
- [lacp failover, page 205](#)
- [lacp fast-switchover, page 207](#)

- [lacp max-bundle, page 209](#)
- [lacp min-bundle, page 211](#)
- [lacp port-priority, page 213](#)
- [lacp rate, page 215](#)
- [lacp system-priority, page 217](#)
- [level \(CFM-AIS-link\), page 219](#)
- [level, page 220](#)
- [lldp, page 221](#)
- [lldp \(interface\), page 224](#)
- [location, page 226](#)
- [location \(interface\), page 227](#)
- [location civic-location identifier, page 229](#)
- [location civic-location-id, page 232](#)
- [location custom-location identifier, page 235](#)
- [location custom-location-id, page 237](#)
- [location geo-location identifier, page 239](#)
- [location geo-location-id, page 241](#)
- [location prefer, page 243](#)

# 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**

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)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.

Release	Modification
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 <fnt> <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|vpn-id}** *vlan-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|vpn-id}** *vlan-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</i> <i>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)SX12	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 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.

**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** {**any**| *vlan-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** {**any**| *vlan-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.
	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.

Command	Description
show ethernet cfm maintenance-points local	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)SX12	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.

**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.

**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
ethernet cfm slm timeout	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
ethernet cfm slm max	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.

**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**

### Syntax Description

<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)

### 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.

### 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

ethernet cfm traceroute cache	Enables caching of Ethernet CFM data learned from traceroute messages.
ethernet cfm traceroute cache size	Sets a maximum number for entries in an Ethernet CFM traceroute cache table.
show running all	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**

### Syntax Description

<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)

### 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.

### 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

Command	Description
<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*

## Syntax Description

<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)

## Command History

Release	Modification
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-evc)#
```

## Related Commands

Command	Description
<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>	<p>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.</p> <p><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.</p>
<i>value</i>	<p>Integer value within ranges that vary depending on the keyword with which it is used. Valid values are as follows:</p> <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
ethernet lmi interface	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)

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** 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
```

Related Commands

Command	Description
ethernet lmi global	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 (#)

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

Command	Description
ethernet loopback local interface	Starts and stops the Ethernet data-plane loopback session on the interface.
show ethernet loopback	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
service instance	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)

Command History	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* ]

### Syntax Description

<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)

### Command History

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.

### 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*

## Syntax Description

<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)

## Command History

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.

Release	Modification
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.
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.
<b>show ethernet oam status</b>	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.

Release	Modification
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.

Release	Modification
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** {**none**| *high-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.

Release	Modification
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

ethernet oam link-monitor on	
	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.



Release	Modification
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.

Release	Modification
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**

## Syntax Description

<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)

## Command History

Release	Modification
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-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**

access-group mode prefer port	Specifies the override modes and the nonoverride modes for an access group and specifies that the PACL mode takes precedence if PACLs are configured.
ethernet oam remote-loopback (interface)	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 master 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**

access-group mode prefer port	Specifies the override modes and the nonoverride modes for an access group and specifies that the PACL mode takes precedence if PACLs are configured.
ethernet oam remote-loopback	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.

### 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*

## Syntax Description

<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)

## 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.

## 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.

Command	Description
service instance (interface)	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 **ethernetsubscriber 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**

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>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**

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>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

<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.

## 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.

Command	Description
event manager applet	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* **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.

## 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.

## 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

<b>vlan-ids</b>	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 <b>,</b> 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.

## 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** form of this command.

**inclusion-list** **vlan-ids** *vlan-id* [*,vlan-range*][*,vlan-range*][*,vlan-range*]

**no inclusion-list** **vlan-ids**

## Syntax Description

<b>vlan-ids</b>	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.

## 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.

# 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.

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



## instance (Ethernet ring)

To create an Ethernet ring instance, use the **instance** command in Ethernet ring configuration mode. To delete the Ethernet ring instance, use the **no** form of this command.

**instance** *instance-id*

**no instance** *instance-id*

### Syntax Description

<i>instance-id</i>	Instance ID. The instance ID can be 1 or 2.
--------------------	---

### Command Default

An Ethernet ring instance is not configured.

### 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.

### Usage Guidelines

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

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

An Ethernet ring can support a maximum of two instances.

### Examples

The following is an example of the **instance** 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)#
```

# 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

<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.
<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)

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.

Release	Modification
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

Command	Description
<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.
<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
show lacp	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**

## Syntax Description

<i>priority</i>	Integer from 1 to 65535 that indicates the priority for the system. 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 system priority is set.

## Command Modes

Global configuration (config)

## 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 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**

### Syntax Description

<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)

### Command History

Release	Modification
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.

## 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>	<p>String that identifies the TLV element to use. Valid values are:</p> <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.
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.

# Ildp (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

med-tlv-select	Selects an LLDP Media Endpoint Discovery (MED) time-length-value (TLV) element to send.
tlv	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>
receive	Enables an interface to receive LLDP transmissions.
transmit	Enables LLDP transmission on an interface.

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

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

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
lldp	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>	<p>The ID for the civic location or the ELIN location. The ID range is from 1 to 4095.</p> <p><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.</p>

### 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.

Release	Modification
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-idid 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**

Command	Description
<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 bgl13  
Device(config-if-port)# city Boston  
Device(config-if-port)# state MA
```

**Related Commands**

Command	Description
<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 bgl15 "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

<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.



## mac access-group in through show ethernet cfm errors

---

- [mac access-group in, page 248](#)
- [mac aging-time, page 250](#)
- [mac limit action flooding disable, page 251](#)
- [mac limit maximum addresses, page 253](#)
- [mac limit maximum addresses \(service instance\), page 254](#)
- [mac security, page 255](#)
- [mac static address, page 259](#)
- [mac tunnel address destination default, page 261](#)
- [mac tunnel address destination map, page 262](#)
- [maximum meps, page 263](#)
- [mep archive-hold-time, page 264](#)
- [mep crosscheck mpid evc, page 266](#)
- [mep crosscheck mpid vlan, page 268](#)
- [mep mpid, page 270](#)
- [mip auto-create, page 271](#)
- [mip auto-create \(cfm-srv\), page 272](#)
- [mlacp interchassis group, page 273](#)
- [mlacp lag-priority, page 274](#)
- [mlacp node-id, page 276](#)
- [mlacp system-mac, page 278](#)
- [mlacp system-priority, page 280](#)
- [monitor loss counter, page 282](#)
- [monitor service instance, page 283](#)

- non-revertive, page 284
- oam protocol, page 285
- open-ring, page 287
- output, page 288
- peer, page 290
- period (CFM-AIS-link), page 292
- ping ethernet, page 293
- ping ethernet evc, page 300
- ping ethernet mpid vlan, page 302
- ping ethernet vlan, page 304
- port0, page 306
- port0 service instance, page 307
- port1, page 308
- port1 service instance, page 309
- port-channel load-balance, page 310
- port-channel load-balance (interface), page 313
- port-channel load-balance mpls, page 315
- port-channel load-balance weighted rebalance, page 317
- priority1, page 319
- priority2, page 320
- profile, page 321
- pseudowire (Layer 2), page 322
- ptp clock, page 324
- rewrite egress tag, page 326
- rewrite ingress tag, page 328
- rpl, page 331
- sender-id, page 332
- sender-id (CFM-srv), page 333
- service (CFM-srv), page 334
- service evc, page 336
- service icc, page 339
- service instance dynamic, page 341
- service instance ethernet, page 343



- [service instance ethernet \(mac-tunnel\), page 346](#)
- [service vlan, page 347](#)
- [service-policy type control policy, page 349](#)
- [show bridge-domain, page 351](#)
- [show cfmpal, page 355](#)
- [show ethernet cfm domain, page 357](#)
- [show ethernet cfm errors, page 360](#)

# mac access-group in

To use a MAC access control list (ACL) to control inbound traffic on an Ethernet service instance, use the **mac access-group in** command in service instance configuration mode. To remove a MAC ACL, use the **no** form of this command.

**mac access-group** *access-list-name* **in**  
**no mac access-group** *access-list-name* **in**

## Syntax Description

<i>access-list-name</i>	Name of a MAC ACL to apply to an interface or subinterface (as specified by the <b>mac access-list extended</b> command).
-------------------------	---

## Command Default

A MAC ACL is not applied to the Ethernet service instance.

## Command Modes

Service instance configuration (config-if-srv)

## Command History

Release	Modification
12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

## Usage Guidelines

The **mac access-group in** command is used to apply MAC ACLs on Ethernet service instances. After a networking device receives a packet, the Cisco IOS software checks the source MAC address of the packet against the ACL. If the MAC ACL permits the address, the software continues to process the packet. If a MAC ACL does not exist on the Ethernet service instance, all packets are passed.

## Examples

The following example shows how to apply a MAC ACL called `mac_layer` on inbound traffic to service instance 100:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# permit 00aa.bbcc.ddee 0.0.0 any
Device(config-ext-macl)# exit
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1q 100
Device(config-if-srv)# mac access-group mac_layer in
```

**Related Commands**

Command	Description
<b>mac access-list extended</b>	Defines a MAC ACL.
<b>show ethernet service instance</b>	Displays information about Ethernet service instances.

## mac aging-time

To set the aging time of MAC addresses in a bridge domain, use the **mac aging-time** command in bridge-domain configuration mode. To remove an aging time setting, use the **no** form of this command.

**mac aging-time** *seconds*

**no mac aging-time**

### Syntax Description

<i>seconds</i>	Aging time, in seconds. The range is from 1 to 600. The default is 300.
----------------	---

### Command Default

If a MAC address aging time is not configured, the default MAC address aging time of 300 seconds is used.

### Command Modes

Bridge-domain configuration (config-bdomain)

### Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

### Usage Guidelines

Use this command if you want to change the aging time of a learned MAC address.

### Examples

The following example shows how to configure an aging time of 25 seconds for MAC addresses in bridge domain 1:

```
Router(config)# bridge-domain 1
```

```
Router(config-bdomain)# mac aging-time 25
```

## mac limit action flooding disable

To prevent flooding (overloading) of a bridge-domain when the maximum number of learned MAC destination addresses is exceeded, use the **mac limit action flooding disable** command in bridge domain configuration mode. To allow flooding, use the **no** form of this command.

**mac limit action flooding disable**

**no mac limit action flooding disable**

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

**Command Default** The flooding is allowed.

**Command Modes** Bridge domain configuration (config-bdomain)

Command History	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 address
- Bridge-domain ID
- Interface type and number
- Service instance number
- Forwarding policy

If the system finds a match (for example, bridge-domain ID), the packets are forwarded to the appropriate interface associated with the bridge domain. If the system does not find a match, copies of the packets are forwarded to each interface associated with the bridge domain. This is known as “flooding.”

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

However, there is a limit to the number of MAC 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 **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 flooding of a bridge-domain when the maximum number of learned MAC destination addresses is exceeded.

```
Device> enable
Device# configure terminal
Device(config)# bridge-domain 100
Device(config-bdmain)# mac limit action flooding disable
```

## mac limit maximum addresses

To set the maximum number of MAC addresses allowed on a bridge domain, use the **mac limit maximum addresses** command in bridge domain configuration mode. To return to the default setting, use the **no** form of this command.

**mac limit maximum addresses** *maximum-addresses*

**no mac limit maximum addresses** [*maximum-addresses*]

### Syntax Description

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

### Command Default

The maximum number of MAC addresses allowed by the device.

### Command Modes

Bridge domain configuration (config-bdomain)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

### Examples

The following example shows how to set the maximum number of MAC addresses on a specific bridge domain to 1000:

```
Device> enable
Device# configure terminal
Device(config)# bridge-domain 100
Device(config-bdomain)# mac limit maximum addresses 1000
```

### Related Commands

Command	Description
<b>mac security maximum addresses</b>	Specifies the maximum number of MAC addresses allowed on an Ethernet service instance.

## mac limit maximum addresses (service instance)

To set the maximum number of MAC addresses allowed on an Ethernet service instance, use the **mac limit maximum addresses** command in service instance configuration mode. To return to the default setting, use the **no** form of this command.

**mac limit maximum addresses** *maximum-addresses*

**no mac limit maximum addresses** [*maximum-addresses*]

### Syntax Description

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

### Command Default

The maximum number of MAC addresses allowed by the device.

### Command Modes

Service instance mode (config-if-srv)

### Command History

Release	Modification
15.3(1)S	This command 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 on an Ethernet service instance to 1000:

```
Device> enable
Device# configure terminal
Device(config)# configure terminal
Device(config)# interface fastethernet0/0
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1q 100
Device(config-if-srv)# bridge-domain
Device(config-if-srv)# mac limit maximum addresses 1000
```



## mac security

To configure MAC security and the various MAC security elements on an Ethernet service instance, use the **mac security** command in service instance configuration mode. To return to the default MAC security setup on the service instance, use the **no** form of this command.

**mac security** [**address** {**permit**|**deny**} *mac-address*] **aging** {**static**|**sticky**} **time** *aging-time* [**inactivity**]}|  
**maximum addresses** *maximum-addresses* [**sticky** [**address** *mac-address*]] **violation** {**protect**|**restrict**}

**no mac security** [**address** {**permit**|**deny**} *mac-address*] **aging** {**static**|**sticky**} **time** *aging-time* [**inactivity**]}|  
**maximum addresses** *maximum-addresses* [**sticky** [**address** *mac-address*]] **violation** {**protect**|**restrict**}

### Syntax Description

address	(Optional) Sets up a MAC address to be permitted or denied.
permit	(Optional) Adds the specified MAC address as a permit MAC address for the Ethernet service instance.
deny	(Optional) Adds the specified MAC address as a deny MAC address for the Ethernet service instance.
mac-address	(Optional) MAC address to be declared a permit or deny MAC address.
<i>aging</i>	(Optional) Sets the aging time of the addresses in the MAC address table.
static	(Optional) Specifies that the mac security <b>aging time</b> <i>aging-time</i> command is also applicable to permitted MAC addresses.  <b>Note</b> The <b>mac security aging time</b> <i>aging-time</i> command sets the aging time of the addresses in the MAC address table to <n> minutes. By default, this affects only dynamically learned addresses--permit addresses are not affected by the application of this command.
sticky	(Optional) Specifies that the <b>mac security aging time</b> command is also applicable to dynamically learned sticky MAC addresses.
time	(Optional) Sets up the aging-time functionality for the MAC security aging operation.
<i>aging-time</i>	(Optional) Aging time of the addresses in the MAC address table, in minutes.

inactivity	(Optional) Specifies that the aging time of <n> minutes be measured from the instant that the MAC address was last encountered on the service instance.
maximum addresses	(Optional) Sets the maximum number of MAC addresses allowed on the Ethernet service instance.
maximum-addresses	(Optional) Maximum number of MAC addresses allowed on the Ethernet service instance.
sticky	(Optional) Enables the “sticky” feature on a secured Ethernet service instance. This means that MAC addresses that are learned dynamically on the Ethernet service instance are kept persistent across line transitions and device reloads.
address	(Optional) Sets up a MAC address to be declared as a sticky MAC address.
mac-address	(Optional) MAC address to be declared as a sticky MAC address.
violation	(Optional) Configures the desired violation response on the Ethernet service instance.  <b>Note</b> If a violation response (protect or restrict) is not configured, the default response is shutdown mode.
protect	(Optional) Configures a protect violation response on the Ethernet service instance.
restrict	(Optional) Configures a restrict violation response on the Ethernet service instance.

**Command Default**

MAC security is disabled.

**Command Modes**

Service instance configuration (config-if-srv)

**Command History**

Release	Modification
12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

The MAC security operation is enabled on an Ethernet service instance by the **mac security** command. Configuring or removing MAC security elements is permitted irrespective of whether MAC security is enabled. Configured elements become operational only when the **mac security** command is issued and MAC security is enabled.

## Examples

The following example shows how to enable MAC security on Ethernet service instance 100:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1q 100
Device(config-if-srv)# bridge-domain 200
Device(config-if-srv)# mac security
```

The following example shows how to configure a MAC address permit with three addresses:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 3/0/1
Device(config-if)# service instance 200 ethernet
Device(config-if-srv)# encapsulation dot1Q 200
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security maximum addresses 3
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaaa
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaab
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaac
Device(config-if-srv)# mac security
```

The following example shows how to enable a MAC address violation protect response on a service instance:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1Q 100
Device(config-if-srv)# bridge-domain 200
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaaa
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaab
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaac
Device(config-if-srv)# mac security violation protect
Device(config-if-srv)# mac security
```

The following example shows how to enable MAC address security aging on a service instance, with the aging time set to 100 minutes:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 3/0/1
Device(config-if)# service instance 200 ethernet
Device(config-if-srv)# encapsulation dot1Q 200
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security aging time 100
Device(config-if-srv)# mac security
```

The following example shows how to configure a MAC address limit of 1000 on a service instance.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# service instance 150 ethernet
Device(config-if-srv)# encapsulation dot1Q 150
```

```
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security maximum addresses 1000
Device(config-if-srv)# mac security
```

The following example shows how to configure sticky MAC addressing on an Ethernet service instance:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1q 100
Device(config-if-srv)# bridge-domain 150
Device(config-if-srv)# mac security sticky
Device(config-if-srv)# mac security
```

## Related Commands

Command	Description
<b>bridge-domain (service instance)</b>	Binds the service instance to a bridge-domain instance.
<b>encapsulation dot1q</b>	Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.
<b>service instance ethernet</b>	Sets up an Ethernet service instance and places the CLI in service instance configuration mode.

## mac static address

To configure a static MAC address, use the **mac static address** command either in service instance configuration mode or in VFI neighbor configuration mode. To remove a static MAC address, use the **no** form of this command.

**mac static address** *mac-addr* [**auto-learn**] [**disable-snooping**]

**no mac static address** *mac-addr*

### Syntax Description

<i>mac-addr</i>	The 48-bit static MAC address.
<b>auto-learn</b>	(Optional) Specifies that when a router detects the same MAC address on a different port, the MAC address entry is to be updated with the new port. <ul style="list-style-type: none"><li>• This keyword is available only for static unicast MAC addresses.</li></ul>
<b>disable-snooping</b>	(Optional) Disables Internet Group Multicast Protocol (IGMP) snooping on the multicast MAC address. <ul style="list-style-type: none"><li>• This keyword is available only for IPv4 and IPv6 static multicast MAC addresses.</li></ul>

### Command Default

MAC static addresses are not configured.

### Command Modes

Service instance configuration (config-if-srv) VFI neighbor configuration (config-vfi-neighbor)

### Command History

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

### Usage Guidelines

Static MAC addresses are related to a Layer 2 bridge domain table; therefore, only bridged services are supported.

Static MAC address configuration is supported only on Ethernet virtual circuit (EVC) bridge domain interfaces and VFI pseudowires.

A unicast static MAC address and MAC security cannot be simultaneously configured on the same Ethernet flow point (EFP). A static MAC multicast address and MAC security can be simultaneously supported on the same EFP.

The number of MAC addresses (unicast and multicast) is limited to 1024 per bridge domain, pseudowire, virtual forwarding instance (VFI), or system.

## Examples

The following example shows how to configure a MAC static address in service instance configuration mode:

```
Router(config)# interface ethernet 1/0
Router(config-if)# service instance 123 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac static address 3333.1111.1111
```

The following example shows how to configure a MAC static address in VFI neighbor configuration mode:

```
Router(config)# 12 vfi foo-core manual
Router(config-vfi)# vpn id 100
Router(config-vfi)# bridge-domain 10
Router(config-vfi)# neighbor 11.0.0.1 pw-class hubclass
Router(config-vfi-neighbor)# mac static address 1111.2222.3333
```

## mac tunnel address destination default

To specify a B-component destination address (B-DA) for a group of service instance IDs (I-SIDs), use the **mac tunnel address destination default** command in MAC-in-MAC tunnel configuration mode. To remove a MAC tunnel address, use the **no** form of this command.

**mac tunnel address destination default** *mac-addr*

**no mac tunnel address destination default** *mac-addr*

### Syntax Description

<i>mac-addr</i>	48-bit MAC address.
-----------------	---------------------

### Command Default

B-DAs are not configured.

### Command Modes

MAC-in-MAC tunnel configuration (config-tunnel-minm)

### Command History

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

### Usage Guidelines

The MAC address specified can be either a unicast or a multicast address.

### Examples

The following example shows how to specify a B-DA using MAC address 3333.1111.1111:

```
Router(config)# ethernet mac-tunnel virtual 1
Router(config-tunnel-minm)# mac tunnel address destination default 3333.1111.1111
```

# mac tunnel address destination map

To map a service provider backbone bridge MAC address to a customer MAC address, use the **mac tunnel address destination map** command in MAC tunnel service configuration mode. To remove a bridge mapping, use the **no** form of this command.

**mac tunnel address destination map** *c-mac-addr b-mac-addr*

**no mac tunnel address destination map** *c-mac-addr b-mac-addr*

## Syntax Description

<i>c-mac-addr</i>	48-bit MAC address of the customer bridge.
<i>b-mac-addr</i>	48-bit MAC address of the service provider bridge.

## Command Default

Service provider and customer bridges are not mapped.

## Command Modes

MAC tunnel service configuration (config-tunnel-srv)

## Command History

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

## Usage Guidelines

The MAC address specified can be either a unicast or a multicast address. If a packet's destination is a backbone edge bridge, the MAC address must be a unicast address.

## Examples

The following example shows how to map a customer bridge to a service provider backbone bridge:

```
Router(config)# ethernet mac-tunnel virtual 1  
Router(config-tunnel-mimn)# service instance 1 ethernet  
Router(config-tunnel-srv)# mac tunnel address destination map 3333.1111.1111 5555.2222.2222
```



## maximum meps

To specify the number of maintenance endpoints (MEPs) across the network in a maintenance association, use the **maximum meps** command in Ethernet connectivity fault management (CFM) service configuration mode. To restore the default value, use the **no** form of this command.

**maximum meps** *max-num*

**no maximum meps**

### Syntax Description

<i>max-num</i>	Integer from 1 to 65535. The default is 100.
----------------	--

### Command Default

A maximum number of MEPs is not configured.

### Command Modes

Ethernet CFM service configuration (config-ecfm-srv)

### 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.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

### Usage Guidelines

When the configured maximum is reached, continuity check messages (CCMs) from other remote MEPs are ignored and a warning message is displayed.

Output of the **show running all** command displays “maximum meps 100” when the default value is configured.

### Examples

The following example shows how to configure a maximum of 50 MEPs:

```
Device(config)# ethernet cfm domain operatorA level 5
Device(config-ecfm)# service vlan-id 5 port
Device(config-ecfm-srv)# maximum meps 50
```

### Related Commands

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

## mep archive-hold-time

To set the amount of time, in minutes, that data from a missing maintenance end point (MEP) is kept in the continuity check database or that entries are held in the error database before they are purged, use the **mep archive-hold-time** command in Ethernet connectivity fault management (CFM) configuration mode. To restore the default number of minutes, use the **no** form of this command.

**mep archive-hold-time** *minutes*

**no mep archive-hold-time** *minutes*

### Syntax Description

<i>minutes</i>	Integer from 1 to 65535 that specifies the number of minutes that data from a missing MEP is kept before it is purged. The default is 100.
----------------	--

### Command Default

The command is enabled, and the archive hold time is set to 100 minutes.

### Command Modes

Ethernet CFM configuration (config-ether-cfm)

### Command Modes

Ethernet CFM configuration (config-ecfm)

### 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)SX12	This command was integrated into Cisco IOS Release 12.2(33)SX12. <ul style="list-style-type: none"> <li>• In this release the command is supported only in CFM IEEE.</li> </ul>
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

When you reset the archive hold time, the new hold time applies only to entries in the database that occur after the reset. Entries made before the hold time was reset are not affected by the change.

Different archive hold times can be set for MEPs in different domains.

**Note**

A missing MEP is a remote MEP that sends a 0 expiration time in its continuity check or a remote MEP whose entry in the local continuity check database expires after it exceeds its lifetime.

In CFM IEEE, output of the **show running all** command displays “mep archive hold-time 100” when the default value is configured.

**Examples**

The following example shows how to set a timeout period of 1000 minutes in CFM D1:

```
Device(config-ether-cfm)# mep archive-hold-time 1000
```

The following example shows how to set a timeout period of 1000 minutes in CFM IEEE:

```
Device(config-ecfm)# mep archive-hold-time 1000
```

**Related Commands**

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

## mep crosscheck mpid evc

To statically define a remote maintenance endpoint (MEP) within a maintenance domain, use the **mep crosscheck mpid evc** command in Ethernet CFM configuration mode. To delete a remote MEP, use the **no** form of this command.

**mep crosscheck mpid** *id* **evc** *evc-name* [**mac** *mac-address*]

**no mep crosscheck mpid** *id* **evc** *evc-name* [**mac** *mac-address*]

### Syntax Description

<i>id</i>	Integer in the range from 0 to 8191 that forms the maintenance point ID (MPID).
<i>evc-name</i>	String that identifies the Ethernet virtual circuit (EVC).
<b>mac</b>	(Optional) Indicates that the MAC address of the MEP is specified.
<i>mac-address</i>	(Optional) MAC address in the format abcd.abcd.abcd.

### Command Default

Remote MEPs are not configured.

### Command Modes

Ethernet CFM configuration (config-ether-cfm)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS 12.2(50)SY.

### Usage Guidelines

The **mep crosscheck mpid evc** command is available on the Cisco 7600 Series Route Switch Processor 720 (RSP 720) and the Cisco 7600 Series Supervisor Engine 720.

Use the **mep crosscheck mpid evc** command to statically configure remote MEPs that are part of a domain. These remote MEPs can be used in the cross-check operation. The cross-check operation works only when local MEPs are configured that correspond to the statically configured remote MEPs.

## Examples

The following example shows how to define a MEP within a maintenance domain with an ID of 20, in EVC evc5, and with MAC address a5a1.a5a1.a5a1:

```
Router(config-ether-cfm)# mep crosscheck mpid 20 evc evc5 mac a5a1.a5a1.a5a1
```

## Related Commands

Command	Description
<b>ethernet cfm domain</b>	Defines a CFM maintenance domain at a particular maintenance level.
<b>ethernet cfm mep crosscheck</b>	Enables cross-checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs.
<b>ethernet cfm mep crosscheck start-delay</b>	Configures the maximum amount of time that a device waits for remote MEPs to come up before the cross-check operation is started.
<b>mep crosscheck mpid vlan</b>	Statically defines a remote MEP within a maintenance domain.
<b>show ethernet cfm maintenance points remote crosscheck</b>	Displays information about remote maintenance points configured statically in a cross-check list.

## mep crosscheck mpid vlan

To statically define a remote maintenance endpoint (MEP) within a maintenance domain, use the **mep crosscheck mpid vlan** command in Ethernet CFM configuration mode. To delete a remote MEP, use the **no** form of this command.

**mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*]

**no mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*]

### Syntax Description

<i>id</i>	Integer in the range from 0 to 8191 that forms the maintenance point ID (MPID).
<i>vlan-id</i>	Integer in the range from 1 to 4094 that identifies the VLAN.
<b>mac</b>	(Optional) Indicates that the MAC address of the MEP is specified.
<i>mac-address</i>	(Optional) MAC address in the format abcd.abcd.abcd.

### Command Default

No remote MEPs are configured.

### Command Modes

Ethernet CFM configuration (config-ether-cfm)

### 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(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

### Usage Guidelines

Use the **mep crosscheck mpid vlan** command to statically configure remote MEPs that are part of a domain. These remote MEPs can be used in the cross-check operation. The cross-check operation only works when local MEPs are configured that correspond to the statically configured remote MEPs.

## Examples

The following example shows how to define a MEP within a maintenance domain with an ID of 20, in VLAN 5, and with MAC address a5a1.a5a1.a5a1:

```
Router(config-ether-cfm)# mep crosscheck mpid 20 vlan 5 mac a5a1.a5a1.a5a1
```

## Related Commands

Command	Description
<b>ethernet cfm domain</b>	Defines a CFM maintenance domain at a particular maintenance level.
<b>ethernet cfm mep crosscheck</b>	Enables cross-checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs.
<b>ethernet cfm mep crosscheck start-delay</b>	Configures the maximum amount of time that a device waits for remote MEPs to come up before the cross-check operation is started.
<b>show ethernet cfm maintenance points remote crosscheck</b>	Displays information about remote maintenance points configured statically in a cross-check list.

# mep mpid

To statically define the maintenance endpoints (MEPs) within a maintenance association, use the **mep mpid** command in Ethernet connectivity fault management (CFM) service configuration mode. To remove MEP definitions, use the **no** form of this command.

**mep mpid** *mpid*

**no mep mpid**

## Syntax Description

<i>mpid</i>	Integer from 1 to 8191 that identifies the MEP.
-------------	---

## Command Default

No MEPs are statically defined.

## Command Modes

Ethernet CFM service configuration (config-ecfm-srv)

## 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.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

## Usage Guidelines

Use this command to manually configure a list of MEPs in a maintenance association. The device logs a warning when a discovered MPID is not on the list of configured MPIDs.

## Examples

The following example shows how to configure a MEP with an ID of 25:

```
Device(config)# ethernet cfm domain operatorA level 5
Device(config-ecfm)# service vlan-id 5 port
Device(config-ecfm-srv)# mep mpid 25
```



## mip auto-create

To enable the automatic creation of a maintenance intermediate point (MIP) at a maintenance domain level, use the **mip auto-create** command in Ethernet connectivity fault management (CFM) configuration mode. To disable the automatic creation of a MIP, use the **no** form of this command.

**mip auto-create [lower-mep-only]**

**no mip auto-create [lower-mep-only]**

### Syntax Description

<b>lower-mep-only</b>	(Optional) Creates a MIP only if there is a MEP for the service in another domain at the next lower active maintenance domain level.
-----------------------	--

### Command Default

MIPs will not be created.

### 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

This command configures the MIP creation policy for members of a maintenance domain to apply for automatically creating a MIP at the domain maintenance level.

If you manually configure a MIP for the maintenance association, it will override the **mip auto-create** command for the MIP for that maintenance association. The **mip auto-create** command also has lower precedence than the MIP creation policy at the maintenance association.

### Examples

The following example shows how to enable the automatic creation of a MIP in the customerA domain at maintenance level 5:

```
Device(config)# ethernet cfm domain customerA level 5
Device(config-ecfm)# mip auto-create
```

## mip auto-create (cfm-srv)

To configure the policy for a maintenance association to dynamically create maintenance intermediate points (MIPs) at the enclosing maintenance domain level, use the **mip auto-create** command in Ethernet connectivity fault management (CFM) service configuration mode. To disable the dynamic creation of a MIP, use the **no** form of this command.

**mip auto-create** [**lower-mep-only**| **none**]

**no mip auto-create** [**lower-mep-only**| **none**]

### Syntax Description

<b>lower-mep-only</b>	(Optional) Creates a MIP only if there is a MEP for the service in another domain at the next lower active maintenance domain level.
<b>none</b>	(Optional) Indicates that MIPs should not be dynamically created.

### Command Default

The default behavior is to defer to the MIP configuration policy of the enclosing maintenance domain.

### Command Modes

Ethernet CFM service configuration (config-ecfm-srv)

### 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.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

### Usage Guidelines

If the **lower-mep-only** or **none** options are not configured, a MIP is created at the maintenance association. This command has lower precedence than the manual configuration of a MIP for a maintenance association. For example, if you manually configure a MIP for a maintenance association, that manual configuration overrides the dynamic configuration from this **mip auto-create** command.

### Examples

The following example shows how to configure the policy for a maintenance association to dynamically create MIPs at the enclosing maintenance domain level:

```
Device(config)# ethernet cfm domain Domain_L5 level 5
Device(config-ecfm)# service cust_500_15 vlan 9
Device(config-ecfm-srv)# mip auto-create
```

## mlacp interchassis group

To specify that the port-channel is a Multi-chassis Link Aggregation Control Protocol (mLACP) port-channel, use the **mlacp interchassis group** command in port-channel interface configuration mode. To return to the default setting, use the **no** form of this command.

**mlacp interchassis group** *group-id*

**no mlacp interchassis group** *group-id*

### Syntax Description

<i>group-id</i>	The <i>group-id</i> should match the configured redundancy group.
-----------------	---

### Command Default

Default behavior is normal single chassis port-channel.

### Command Modes

Port-channel interface configuration (config-if)

### Command History

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

### Usage Guidelines

The **mlacp interchassis group** command enables Multi-chassis LACP on the port-channel and specifies the interchassis group to which the port-channel belongs.

### Examples

This example shows how to specify that interchassis group 1 is an mLACP group:

```
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>interface port-channel</b>	Creates a port-channel virtual interface and puts the CLI in interface configuration mode.

# mlacp lag-priority

To set the Link Aggregation Control Protocol (LACP) port priorities for each of the local member links in the Link Aggregation Group (LAG), use the **mlacp lag-priority** command in interface configuration mode. To disable the LACP port priorities, use the **no** form of this command.

**mlacp lag-priority** *priority-value*

**no mlacp lag-priority**

## Syntax Description

<i>priority-value</i>	Integer from 1 to 65535 that defines the port priority. If you enter the command without a priority value, 32768 is used.
-----------------------	---

## Command Default

This command is disabled. LACP port priorities are not set.

## Command Modes

Interface configuration (config-if)

## Command History

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

## Usage Guidelines

Port priority determines which ports should be activated and which should be left in standby mode when there are hardware or software limitations on the maximum number of links allowed in a LAG. For multichassis operation in active/standby mode, the port priorities for all links connecting to the active point of attachment (PoA) must be higher than the port priorities for links connecting to the standby PoA. For example, select the PoA with the highest port priority to be the active PoA, and dynamically adjust the priorities of all other links with the same key to an equal value.



### Note

A numerically lower-priority value equates to a higher LACP priority. The active PoA should be specified by configuring the numerically lower LACP priority value.

This command is used to force a failover during operation in the following two ways:

- Set the active PoA's LAG priority to a value greater than the LAG priority on the standby PoA. This results in the quickest failover because it requires the fewest LACP link state transitions on the standby links before they turn active.
- Set the standby PoA's LAG priority to a value numerically less than the LAG priority on the active PoA. This results in a slightly longer failover time due to standby links having to signal OUT\_OF\_SYNC to the dual-homed device (DHD) before the links can be brought up and go active.

In some cases the operational priority and the configured priority may differ when dynamic port priority management is used to force failovers. In this case, the configured version will not be changed unless the port channel is operating in the “nonrevertive” state. Enter the **show lacp multi-chassis port-channel** command to view the current operational priorities. Enter the **show running-config** command to view the configured priority values.

Dynamic port priority changes are not automatically written back to the running configuration or NVRAM configuration. If you want the current priorities to be used when the system reloads, the **mlacp lag-priority** command must be used and the configuration must be saved.

### Examples

The following example shows how to set the mLACP LAG priority to 1000:

```
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>interface port-channel</b>	Creates a port-channel virtual interface and enters interface configuration mode.

## mlacp node-id

To define the node ID used in the Link Aggregation Control Protocol (LACP) port-ID field by a member of the Multichassis LACP (mLACP) redundancy group, use the **mlacp node-id** command in interchassis redundancy configuration mode. To remove the node ID, use the **no** form of this command.

**mlacp node-id** *node-id*

**no mlacp node-id** *node-id*

### Syntax Description

<i>node-id</i>	Integer from 0 to 7.
----------------	----------------------

### Command Default

A node ID is not defined.

### Command Modes

Interchassis redundancy configuration (config-r-ic)

### Command History

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

### Usage Guidelines

The node ID should be different from the peer IDs.

The **mlacp node-id** command is mandatory to enable mLACP on an interchassis group.

### Examples

The following example shows how to define the mLACP node ID as 1 for interchassis group 1 in the redundancy group:

```
redundancy
interchassis group 1
protocol iccp
member ip 1.1.1.1
monitor peer route-watch
backbone interface GigabitEthernet6/1
mlacp node-id 1
mlacp system-mac 1298.acfd.3bc5
mlacp system-priority 100
```

### Related Commands

Command	Description
<b>interchassis group</b>	Configures an interchassis group in interchassis redundancy configuration mode and assigns a group number.

Command	Description
redundancy	Enters interchassis redundancy configuration mode.

## mlacp system-mac

To define and advertise the system MAC address to the Multichassis Link Aggregation Control Protocol (mLACP) members of the redundancy group for arbitration, use the **mlacp system-mac** command in interchassis redundancy configuration mode. To disable the advertising of the system MAC address, use the **no** form of this command.

**mlacp system-mac** *mac-address*

**no mlacp system-mac** *mac-address*

### Syntax Description

<i>mac-address</i>	MAC address in aabb.ccdd.eeff format.
--------------------	---------------------------------------

### Command Default

The default value used for arbitration is the chassis backplane MAC address.

### Command Modes

Interchassis redundancy configuration (config-r-ic)

### Command History

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

### Usage Guidelines

The lowest numerical MAC address in the specified interchassis group will be used by the mLACP.

### Examples

The following example shows how to set the MAC address 1298.acfd.3bc5 to be advertised to the mLACP members of interchassis group 1 in the redundancy group for arbitration:

```
redundancy
interchassis group 1
 protocol iccp
 member ip 10.1.1.1
 monitor peer route-watch
 backbone interface GigabitEthernet6/1
 mlacp node-id 1
 mlacp system-mac 1298.acfd.3bc5
 mlacp system-priority 100
```

### Related Commands

Command	Description
<b>interchassis group</b>	Configures an interchassis group within the interchassis redundancy configuration mode and assigns a group number.



Command	Description
<b>redundancy</b>	Enters interchassis redundancy configuration mode.

# mlacp system-priority

To define the system priority to be advertised to other members of the Multichassis Link Aggregation Control Protocol (mLACP) redundancy group for arbitration, use the **mlacp system-priority** command in interchassis redundancy configuration mode. To return the system priority to the default value, use the **no** form of this command.

**mlacp system-priority** *priority-value*  
**no mlacp system-priority**

## Syntax Description

<i>priority-value</i>	Integer from 1 to 65535 that is the priority for the physical interfaces. The default is 32768.
-----------------------	---

## Command Default

The default value for the system priority is set to 32768.

## Command Modes

Interchassis redundancy configuration (config-r-ic)

## Command History

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

## Usage Guidelines

Each device that runs the mLACP has an mLACP system priority value. You can accept the default value of 32768 for this parameter, or you can configure a value between 1 and 65535. The mLACP uses the system priority with the MAC address to form the system ID and also during negotiation with other systems. The system ID is unique for each virtual device context (VDC).

When setting the priority, note that a higher number means a lower priority.

This command does not require a license.

## Examples

The following example shows how to set the system priority to 100 for interchassis group 1 in the redundancy group for arbitration:

```

redundancy
 interchassis group 1
  protocol iccp
  member ip 10.1.1.1
  monitor peer route-watch
 backbone interface GigabitEthernet6/1
  mlacp node-id 1
  mlacp system-mac 1298.acfd.3bc5
  mlacp system-priority 100

```

**Related Commands**

Command	Description
<b>interchassis group</b>	Configures an interchassis group in the interchassis redundancy configuration mode and assigns a group number.
<b>redundancy</b>	Enters interchassis redundancy configuration mode.

# monitor loss counter

To monitor local Tx and Rx aggregated counters for losses, use the **monitorlosscounter** command in Ethernet CFM interface configuration mode. To turn off monitoring, use the **no** form of this command.

**monitor loss counter** [*priority cos-range*]

**no monitor loss counter**

## Syntax Description

<b>priority</b>	(Optional) Monitors local Tx and Rx counters for loss functionality.
<i>cos-range</i>	(Optional) String that identifies the class of service.

## Command Default

Counters are not maintained when this command is not configured.

## Command Modes

Ethernet CFM interface configuration (config-if-ecfm-mep)

## Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

## Usage Guidelines

An aggregate counter includes both the Tx and Rx counters for all traffic matching an Ethernet flow point (EFP) and for all class-of-service (CoS) values defined by the **encapsulation** command, when a priority is not defined by the **monitorlosscounter** command. If a priority is defined by the **monitorlosscounter** command, separate Rx and Tx counters are maintained for each priority defined.

## Examples

The following example shows how to configure monitoring for loss counters:

```
Device(config)# ethernet cfm domain test level 5
Device(config-ecfm)# service vlan-id 17
Device(config-ecfm-srv)# exit
Device(config-ecfm)# exit
Device(config)# interface gigabitethernet 1/1
Device(config-if)# ethernet cfm mep domain test mpid 5 vlan 17
Device(config-if-ecfm-mep)# monitor loss counter
```

## monitor service instance

To assign an Ethernet service instance used to monitor the ring port, use the **monitor service instance** command in the Ethernet ring port configuration mode. To remove the assignment, use the **no** form of this command.

**monitor service instance** *instance-id*

**no monitor service instance**

### Syntax Description

<i>instance-id</i>	Instance ID. Valid entries are numbers in the range of 1 to 4000.
--------------------	---

### Command Default

An Ethernet ring instance is not assigned to monitor the ring port.

### Command Modes

Ethernet ring port configuration (config-erp-ring-port)

### 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.

### Usage Guidelines

The port being monitored can be either port0 or port1. Assigning a service instance to monitor the ring port is optional. Monitoring can also be achieved by using Connectivity Fault Management (CFM) and maintenance endpoints (MEPs).

### Examples

The following is a sample configuration in which the **monitor service instance** command has been enabled to monitor the port. In this example, the ring port being monitored is port0.

```
Device> enable
Device# configure terminal
Device(config)# ethernet ring g8032 ring1
Device(config-erp-ring)# port0 interface fastethernet 0/0/1
Device(config-erp-ring-port)# monitor service instance 1
Device(config-erp-ring-port)# end
```

## non-revertive

To specify a ring instance as non-revertive, use the **non-revertive** command in Ethernet ring configuration mode. To remove this specification, use the **no** form of this command.

**non-revertive**

**no non-revertive**

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

**Command Default** By default, ring instances are revertive.

**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.

**Examples** The following is an example of the **non-revertive** command used in an Ethernet ring configuration.

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

## oam protocol

To specify an operations, maintenance, and administration (OAM) protocol for an Ethernet virtual connection (EVC), use the **oam protocol** command in EVC configuration mode. To remove an OAM protocol configuration for an EVC, use the **no** form of this command.

**oam protocol** {**cfm** *svlan* *svlan-id* **domain** *domain-name*| **ldp**}

**no oam protocol**

### Syntax Description

<b>cfm</b>	Specifies Connectivity Fault Management (CFM) as the protocol.
<b>svlan</b>	Specifies a service provider VLAN.
<i>svlan-id</i>	Integer in the range of 1 to 4094 that identifies the service provider VLAN.
<b>domain</b>	Specifies a CFM maintenance domain.
<i>domain-name</i>	String of a maximum of 256 characters that identifies the domain.
<b>ldp</b>	Specifies Label Distribution Protocol (LDP).

### Command Default

An OAM protocol is not specified.

### Command Modes

EVC configuration (config-evc)

### Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

### Usage Guidelines

Use this command to specify the OAM protocol to use for communicating link status in an Ethernet over Multiprotocol Label Switching (EoMPLS) network.

## Examples

The following example shows how to specify CFM as the OAM protocol:

```
Device(config)# ethernet evc evc10  
Device(config-evc)# oam protocol cfm svlan 10 domain cstmr
```



# open-ring

To specify an Ethernet ring as an open ring, use the **open-ring** command in Ethernet ring configuration mode. To remove the specification, use the **no** form of this command.

**open-ring**

**no open-ring**

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

**Command Default** The Ethernet ring is not specified as an open ring.

**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.

**Usage Guidelines** The command evaluates whether the Automatic Protection Switching (APS) channel is an open or closed ring. If the APS channel is an open ring, the Ethernet Ring Protection (ERP) protocol always allows Ring Automatic Protection Switching (R-APS) messages to be sent, but data traffic may be blocked by the ERP process.

This command must be configured on every node in the open ring, not just on the endpoints of the ring.

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

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

# output

To enable out put of time of day messages using a 1PPS interface, use the **output** command in global configuration mode. To disable PTP output, use the **no** form of this command.

**output 1pps slot/bay [offset offset-value [negative]] [pulse-width pulse-amount {ns| us| ms}]**

**no output 1pps slot/bay [offset offset-value [negative]] [pulse-width pulse-amount {ns| us| ms}]**

## Syntax Description

<b>1pps</b>	Configures the device to send 1 packet per second (1PPS) time of day messages using the RS422 port or 1PPS port. You can select 1PPS output with or without selecting a timing port.
<i>slot</i>	Slot of the 1PPS interface.
<i>bay</i>	Bay of the 1PPS interface.
<b>offset</b>	(Optional) Specifies an offset to compensate for a known phase error such as network asymmetry.
<i>offset-value</i>	Amount of offset in nanoseconds. The range is from 0 to 500,000,000.
<b>negative</b>	Specifies a negative offset 1PPS output value.
<b>pulse-width</b>	(Optional) Specifies a pulse width value.
<i>pulse-amount</i>	Amount of the pulse width. The range is from 1 to 4096. For 1PPS output using the RS422 port, you must specify a value of at least 2 ms.
<b>ns</b>	Specifies a pulse width value in nanoseconds.
<b>us</b>	Specifies a pulse width value in microseconds.
<b>ms</b>	Specifies a pulse width value in milliseconds.

## Command Default

Time of day message output 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.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines**

If you want to provide output frequency clock, configure this command in PTP slave mode. This command only applies to platforms that have 1PPS ports.

**Examples**

The following example shows how to configure output clocking:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# output 1pps 3/0 offset 10 pulse-width 1000 ms
Device(config-ptp-clk)# end
```

The following example shows the time of day (ToD) configuration on the 1588V2 slave and corresponding output:

```
Device> enable
Device# config terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# tod 3/3 cisco
Device(config-ptp-clk)# output 1pps 0 250 ns
Device(config-ptp-clk)# clock-port SLAVE slave
```

**Related Commands**

Command	Description
<b>input</b>	Enables PTP input clocking using the 1.544 Mhz, 2.048 Mhz, or 10 Mhz timing interface or phase using the 1PPS or RS-422 interface.

## peer

To define the target label distribution protocol (LDP) peer provider edge (PE) information, use the **peer** command in Layer 2 (L2) subscriber group command mode. To disable the information configured for the target LDP peer, use the **no** form of this command.

**peer** {**host** *destination-host-address*|**network** *destination-network-address destination-network-mask*} *vc-id* [*vc-id-range*]

**no peer** {**host** *destination-host-address*|**network**}

### Syntax Description

<b>host</b> <i>destination-host-address</i>	Specifies the target LDP destination host address of the peer PE device that belongs to the authorization group.
<b>network</b> <i>destination-network-address destination-network-mask</i>	Specifies the target LDP destination network address and network mask of the peer PE devices that belong to the authorization group.
<i>vc-id</i>	Virtual circuit (VC) ID of the peer PE device. Valid values are from 1 to 4294967295.
<i>vc-id-range</i>	(Optional) Upper range for the VC ID. Valid values are from 1 to 4294967295.

### Command Default

Target LDP peer PE device information is not configured and label bindings are not advertised.

### Command Modes

L2 subscriber group configuration (config-l2-sub-gr)

### Command History

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

### Usage Guidelines

You can use the **peer** command to define the target Any Transport over MPLS (ATOM) LDP peer information. The target LDP peer sends LDP virtual circuit (VC) advertisements in an MPLS aggregation network.

When an LDP VC label advertisement message arrives, if there is no xconnect configured, based on the host address, the network address, and the VC ID of the peer, an attempt to identify a service authorization group is made. The message is treated as a First Sign of Life (FSOL) only when a match is found for the message, and a request is sent to the policy plane for subscriber authorization. However, if no match is found, no subscriber authorization will be attempted.

When a label withdraw message is received, the system checks if a corresponding xconnect is already created. If the xconnect is found, it will be removed. Xconnect will not be destroyed in response to a pseudowire status message.

You must be sure to define mutually exclusive service authorization groups. Within a router, the *destination-host-address* and *vc-id-range* combination must be unique to identify a unique service authorization group.

## Examples

The following example shows how to configure the host information for a peer PE device with a VC ID range:

```
Router# configure terminal
Router(config)# l2 subscriber authorization group group1
Router(config-l2-sub-gr)# peer host 10.10.1.1 23 54
```

## Related Commands

Command	Description
<b>l2 subscriber</b>	Creates an L2 subscriber authorization group and enters L2 subscriber group mode.
<b>pseudowire (Layer 2)</b>	Defines the maximum and watermark limits for a 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.

## period (CFM-AIS-link)

To configure a specific Alarm Indication Signal (AIS) transmission interval on a server maintenance endpoint (SMEP), use the **period** command in CFM SMEP AIS configuration mode. To remove the interval configuration, use the **no** form of this command.

**period** *seconds*

**no period**

### Syntax Description

<i>seconds</i>	Integers 1 or 60 that specify the time interval, in seconds, between AIS transmissions. The default is 60.
----------------	--

### Command Default

AIS frames are transmitted every 60 seconds.

### Command Modes

CFM SMEP AIS configuration mode (config-ais-link-cfm)

### Command History

Release	Modification
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

When the default value is configured, “period 60” is displayed when the **show running all** command is issued.

### Examples

The following example shows how to configure an AIS transmission interval of 1 second:

```
Device(config)# ethernet cfm ais link-status global
Device(config-ais-link-cfm)# period 1
```

### Related Commands

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

## ping ethernet

To send Ethernet connectivity fault management (CFM) loopback messages to a destination maintenance endpoint (MEP) and maintenance intermediate point (MIP), use the **ping ethernet** command in privileged EXEC mode.

**ping ethernet** {*mac-address*| **mpid** *mpid*| **multicast**} **domain** *domain-name* {**port**| **service** **icc** *icc-code* *meg-id*} [**cos** *cos-value*| **source** *source-mpid* [**cos** *cos-value*]] [**de**]

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

**ping ethernet** {*mac-address*| **mpid** *mpid*| **multicast**} **domain** *domain-name* **service** {*short-ma-name*| **icc** *icc-code* *meg-id*| **number** *ma-number*| **vlan-id** *vlan-id*| **vpn-id** *vpn-id*} [**cos** *cos-value*| **source** *source-mpid* [**cos** *cos-value*]] [**de**] [**pad** {*data-pattern*| **test** *pattern-type* *pattern-value*} **validate**]

### Cisco ASR 901 Series Aggregation Services Routers

**ping ethernet**{*mac-address*| **mpid** *mpid*} {**domain** *domain-name*{**vlan** *vlan-id* [**source** *source-mpid*] **level** *level-id*{**vlan** *vlan-id*} }}

#### Syntax Description

<i>mac-address</i>	MAC address of the destination MEP in the format abcd.abcd.abcd.
<b>mpid</b> <i>mpid</i>	Specifies a MEP identifier (MPID) and value. Range: 1 to 8191.
<b>multicast</b>	Specifies a multicast loopback message.
<b>domain</b> <i>domain-name</i>	Specifies the domain where the destination MEP resides. Maximum: 154 characters.
<b>port</b>	Specifies a port MEP.
<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</i> <i>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.
<b>cos</b> <i>cos-value</i>	<p>(Optional) Specifies a class of service (CoS) for a MEP that will be sent in Ethernet CFM messages. CoS value range: 0 to 7.</p> <ul style="list-style-type: none"> <li>• ICC (maximum: 6 characters) and UMC (maximum: 12 characters).</li> <li>• The default is retrieved from the MEP identified by the MPID if the <b>cos</b> keyword is not configured. If the <b>mpid</b> keyword is not configured, the default is the highest priority on the egress interface.</li> </ul>
<b>source</b> <i>source-mpid</i>	(Optional) Specifies an MEP's CoS that will be sent in Ethernet CFM messages. Source MPID value range: 1 to 819.
<b>de</b>	(Optional) Specifies whether the packet is drop-eligible. The <b>de</b> option is platform-dependent.
<b>pad</b>	(Optional) Specifies padding data type, length, value (TLV) .
<i>data-pattern</i>	(Optional) The data pattern of data TLV in hexadecimal format.
<b>test</b>	(Optional) Specifies test TLV.
<b>pattern-type</b> <i>pattern-value</i>	<p>(Optional) Specifies a pattern type for loopback messages, allowing you to use Test TLV in one-line command format. Pattern value for loopback messages:</p> <ul style="list-style-type: none"> <li>• 0: Null signal without CRC-32</li> <li>• 1: Null signal with CRC-32</li> <li>• 2: PRBS 2 (-31) without CRC-32</li> <li>• 3: PRBS 2 (-31) with CRC-32</li> </ul>
<b>validate</b>	(Optional) Specifies that the reply data is validated.
<b>level</b>	Indicates that a maintenance level is specified.
<i>level-id</i>	Number from 0 to 7 that indicates the maintenance level.



**Command Default** A CFM ping operation to the specified MEP and MIP is performed.

**Command Modes** Privileged EXEC (#)

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.
	15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
	15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The <b>service icc</b> keyword was added to provide support for the ICC-based MEG identifier.
	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. <ul style="list-style-type: none"> <li>• Support for ITU-T Y.1731 CFM Test TLV was added.</li> <li>• The <b>port</b> keyword was deprecated and options to specify the MA service via the <b>service</b> keyword were introduced.</li> </ul>
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines**

Use this command to test connectivity between MEPs.

If the continuity check database does not have entries for the specified MPID, an error message is displayed notifying you to use the **ping ethernet mac-address** command instead.

If a domain name is more than 154 characters in length, a warning message is displayed notifying you that the maintenance domain ID (MDID) will be truncated to 43 characters in continuity check messages (CCMs) if "id <fmt> <MDID>" is not configured.

This command can be issued by specifying keywords and arguments as one command or as an extended command in which you specify options line by line.

The CFM ping (loopback) supports up to 1488 bytes.

In Cisco IOS XE Release 3.7S and later releases, support for ITU-T Y.1731 CFM Test TLV allows you to specify one of four pattern values for loopback messages:

- 0: Null signal without 32-bit cyclic redundancy check codes (CRC-32)
- 1: Null signal with CRC-32
- 2: Pseudorandom bit sequences (PRBS) 2 (-31) without CRC-32

- 3: PRBS 2 (-31) with CRC-32

Null signal means padding 0 for the payload of the Test TLV.

You can initiate the loopback message with Test TLV either by specifying the **pad test pattern-type** keyword in the one-line command format or using the extended command format, as shown in the examples.

You can also use Test TLV to validate the packet data on the initiator side.

For Cisco ASR 901 Series Aggregation Services Routers, if a domain name has more than 43 characters, a warning message is displayed notifying you that the maintenance domain ID (MDID) will be truncated to 43 characters in continuity check messages (CCMs) if "id <fmt> <MDID>" is not configured.

## Examples

The following example shows how to send an Ethernet CFM loopback message to a destination MEP using the extended command format:

```
Device# ping

Protocol [ip]: ethernet
Multicast [n] :
Mac Address : 0015.6215.46d0
Maintenance Domain : vik-vfi-ofm
Use short-MA-name [n]: y
Short-MA-name format(text, vlan-id, number, vpn-id) [text]:
Short-MA-name: zzz
Source MPID [555]:
Repeat Count [5]:
Datagram Size [100]: 9000
% A decimal number between 64 and 1488.
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]:
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 0015.6215.46d0, timeout is 5 seconds:!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

Device# ping

Protocol [ip]: ethernet
Multicast [n] :
Mac Address : 0015.637b.4e00
Maintenance Domain : CUSTOMER
Use short-MA-name [n]: y
Short-MA-name format(text, vlan-id, number, vpn-id) [text]:
Short-MA-name: zzz
Source MPID [2345]:
Repeat Count [5]:
Datagram Size [100]: 9000
% A decimal number between 64 and 1488.
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]:
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 0015.637b.4e00, timeout is 5 seconds:!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

The table below describes the significant fields in the display.
```

**Table 1: ping ethernet Field Descriptions**

Field	Description
Protocol [ip]	Protocol name. The value within the brackets indicates the default value. If no value is specified, the default is considered.
Multicast [n]	Specifies a multipoint address. The value within the brackets indicates the default value. If no value is specified, the default is considered.
MAC Address	MAC address of the interface.
Maintenance Domain	Specifies the maintenance domain.
Short-MA-name	Specifies the short MA name.
Source MPID [555]	Specifies a maintenance point identifier. The value within the brackets indicates the default value (555).
Repeat Count [5]	Number of ping packets that are sent to the destination address. The value within the brackets indicates the default value (5).
Datagram Size [100]	Size of the ping packet (in bytes). The value within the brackets indicates the default value (100).
Timeout in seconds [5]	Timeout (in seconds). The ping is declared successful only if the ECHO REPLY packet is received before the time interval. The value within the brackets indicates the default value (5).
Interval in seconds [0]	Timeout interval (in seconds). The value within the brackets indicates the default value (0).
Extended commands	Specifies whether a series of additional commands appears.

The following example shows how to initiate a loopback message with Test TLV using a one-line command that specifies pattern type 0: NULL signal without CRC-32:

```
Device# ping ethernet mpid 2 domain yyy service zzz pad test pattern-type 0
```

Type escape sequence to abort.

Packet sent with test TLV type 0: NULL signal without CRC-32

Sending 5 Ethernet CFM loopback messages to aabb.cc00.6500, timeout is 5 seconds:!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

The following example shows how to initiate a loopback message using the extended command format and not specifying Test TLV:

```
Device# ping
```

Protocol [ip]: ethernet

Multicast [n]:

Mac Address: aabb.cc00.6500

Maintenance Domain: yyy

```

Use short-MA-name [n]: y
Short-MA-name format(text, vlan-id, number, vpn-id) [text]:
Short-MA-name: zzz
Source MPID [1]:
Repeat Count [5]:
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]: y
Class of Service [2]:
Set DE bit? [no]:
Validate reply data? [no]:
Test TLV? [no]:
Data pattern [0xABCD]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Packet has data pattern 0xABCD
Sending 5 Ethernet CFM loopback messages to aabb.cc00.6500, timeout is 5 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

```

The following example shows how to initiate a loopback message using the extended command format and specifying Test TLV and pattern type 1: NULL signal with CRC-32:

```

Device# ping

Protocol [ip]: ethernet
Multicast [n]:
Mac Address: aabb.cc00.6500
Maintenance Domain: yyy
Use short-MA-name [n]: y
Short-MA-name format(text, vlan-id, number, vpn-id) [text]:
Short-MA-name: zzz
Source MPID [1]:
Repeat Count [5]:
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]: y
Class of Service [2]:
Set DE bit? [no]:
Validate reply data? [no]:
Test TLV? [no]: yes
Pattern Type (0: NULL, 1: PRBS) [0]: 0
Pattern Type with CRC? [no]: yes
Sweep range of sizes [n]:
Type escape sequence to abort.
Packet sent with test TLV type 1: NULL signal with CRC-32
Sending 5 Ethernet CFM loopback messages to aabb.cc00.6500, timeout is 5 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

```

The following example shows how to initiate a loopback message using the extended command format, specifying Test TLV and pattern type 3: PRBS 2(-31) with CRC-32, and also specifying that the packet is validated:

```

Device# ping

Protocol [ip]: ethernet
Multicast [n]:
Mac Address: aabb.cc00.6500
Maintenance Domain: yyy
Use short-MA-name [n]: y
Short-MA-name format(text, vlan-id, number, vpn-id) [text]:
Short-MA-name: zzz
Source MPID [1]:
Repeat Count [5]:
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]: y
Class of Service [2]:

```

```
Set DE bit? [no]:
Validate reply data? [no]: yes
Test TLV? [no]: yes
Pattern Type (0: NULL, 1: PRBS) [0]: 1
Pattern Type with CRC? [no]: yes
Sweep range of sizes [n]:
Type escape sequence to abort.
Packet sent with test TLV type 3: PRBS 2^(-31) with CRC-32
Reply data will be validated
Sending 5 Ethernet CFM loopback messages to aabb.cc00.6500, timeout is 5 seconds:!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The following examples show how to send an Ethernet CFM loopback message to a destination MEP using the "extended ping" format for Cisco ASR 901 Series Aggregation Services Routers:

Router# **ping**

```
Protocol [ip]: ethernet
Mac Address : aabb.cc03.bb99
Maintenance Domain : Domain_L5
VLAN [9]:
Source MPID [220]:
Repeat Count [5]:
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]:
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to aabb.cc03.bb99, timeout is 5 seconds:!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Router# **ping**

```
Protocol [ip]: ethernet
Multicast [n] : y
Maintenance Domain : Domain_L5
VLAN [9]:
Source MPID [220]:
Datagram Size [100]:
Timeout in seconds [5]:
Interval in seconds [0]:
Extended commands [n]:
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 0180.c200.0035, timeout is 5 seconds:
Reply to Multicast request from aabb.cc03.bb99, 0 ms
Total Remote MEPs replied: 1
```

## ping ethernet evc

To send Ethernet connectivity fault management (CFM) loopback messages to a maintenance endpoint (MEP) or maintenance intermediate point (MIP) destination, use the **ping ethernet evc** command in privileged EXEC mode.

**ping ethernet** {*mac-address*| *mpid*} {**domain** *domain-name*| **level** *level-id*} **evc** *evc-name* [**cos** *cos-value*| **source** *mpid*]

### Syntax Description

<i>mac-address</i>	MAC address of the remote maintenance point in the format abcd.abcd.abcd.
<i>mpid</i>	Integer from 0 to 8191 that identifies the MEP.
<b>domain</b>	Indicates a domain is specified.
<i>domain-name</i>	String with a maximum of 154 characters that identifies the domain.
<b>level</b>	Indicates that a maintenance level is specified.
<i>level-id</i>	Integer from 0 to 7 that identifies the maintenance level.
<i>evc-name</i>	String that identifies the Ethernet virtual circuit (EVC).
<b>cos</b> <i>cos-value</i>	Specifies the class of service (cos) and the value for the cos. Integer from 0 to 7 that identifies the value for cos.
<b>source</b> <i>mpid</i>	(Optional) Indicates a source maintenance point.

### Command Default

A basic CFM ping operation to the specified MAC address (MEP or MIP) is performed.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(50)SY	This command was integrated.

### Usage Guidelines

A local MEP must be configured for the same level and EVC before you can use this command.

The optional **source** keyword is available only when you enter a domain name. The **source** keyword is useful when there are multiple local MEPs in the same domain, level, and EVC as the ping target. For outward facing MEPs, choosing the source MPID implicitly selects the interface from which the ping will be sent.

### Examples

The following example shows how to send an Ethernet CFM loopback message to MAC address 1010.pcef.1010 at maintenance level 2 on evc5:

```
Router# ping ethernet 1010.pcef.1010 level 2 evc evc5
```

### Related Commands

Command	Description
<b>ping</b>	Sends an echo request packet to an address, and then awaits a reply to determine whether a device can be reached or is functioning.
<b>ping ethernet vlan</b>	Sends Ethernet CFM loopback messages to a MEP or MIP destination.

# ping ethernet mpid vlan



**Note**

Effective with Cisco IOS Release 12.4(11)T, the **ping ethernet mpid vlan** command is replaced by the **ping ethernet vlan** command. See the **ping ethernet vlan** command for more information.

To send Ethernet connectivity fault management (CFM) loopback messages to a maintenance endpoint (MEP) destination, use the **ping ethernet mpid vlan** command in privileged EXEC mode.

**ping ethernet mpid** *mpid* {**domain** *domain-name*| **level** *level-id*} **vlan** *vlan-id*

**Syntax Description**

<i>mpid</i>	Integer from 0 to 8191 that identifies the MEP.
<b>domain</b>	Indicates a domain where the destination MEP resides is specified.
<i>domain-name</i>	String with a maximum of 154 characters that identifies the domain.
<b>level</b>	Indicates a maintenance level is specified.
<i>level-id</i>	Integer from 0 to 7 that identifies the maintenance level.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the VLAN.

**Command Default**

A basic CFM ping operation to the specified maintenance endpoint ID (MPID) is performed.

**Command Modes**

Privileged EXEC (#)

**Command History**

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(11)T	This command was replaced by the <b>ping ethernet vlan</b> command.
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**

Use this command to test connectivity between MEPs.

If the continuity check database does not have entries for the specified MPID, an error message displays indicating that the command cannot be used.

**Examples**

The following example shows how to send an Ethernet CFM loopback message to MPID 3075, maintenance domain operatorv, maintenance level 3, VLAN ID 4325:

```
Device# ping ethernet mpid 3075 domain operatorv level 3 vlan 4325
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/62/72 ms
```

**Related Commands**

Command	Description
<b>ping</b>	Sends an echo request packet to an address, and then awaits a reply to determine whether a device can be reached or is functioning.
<b>ping ethernet vlan</b>	Sends Ethernet CFM loopback messages to a destination MAC address.

## ping ethernet vlan

To send Ethernet connectivity fault management (CFM) loopback messages to a maintenance endpoint (MEP) or maintenance intermediate point (MIP) destination, use the **ping ethernet vlan** command in privileged EXEC command mode.

**ping ethernet** {*mac-address*| *mpid*} {**domain** *domain-name*| **level** *level-id*} **vlan** *vlan-id* [**source** *mpid*]

### Syntax Description

<i>mac-address</i>	MAC address of the remote maintenance point in the format abcd.abcd.abcd.
<i>mpid</i>	Integer from 0 to 8191 that identifies the MEP.
<b>domain</b>	Indicates a domain is specified.
<i>domain-name</i>	String with a maximum of 154 characters that identifies the domain.
<b>level</b>	Indicates that a maintenance level is specified.
<i>level-id</i>	Integer value of 0 to 7 that identifies the maintenance level.
<i>vlan-id</i>	Integer value of 1 to 4094 that identifies the VLAN.
<b>source</b> <i>mpid</i>	(Optional) Indicates a source maintenance point.

### Command Default

A basic CFM ping operation to the specified MAC address (MEP or MIP) is performed.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(11)T	The optional <b>source</b> keyword and <i>mpid</i> argument were added in Cisco IOS Release 12.4(11)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.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Release	Modification
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

A local MEP must be configured for the same level and VLAN before you can use this command.

The optional **source** keyword is available only when you enter a domain name. The **source** keyword is useful when there are multiple local MEPs in the same domain, level, and VLAN as the ping target. For outward facing MEPs, choosing the source MPID implicitly selects the interface from which the ping will be sent.

### Examples

The following example shows how to send an Ethernet CFM loopback message to MAC address 4123.pcef.9879 at maintenance level 3, VLAN ID 4325:

```
Device# ping ethernet 4123.pcef.9879 level 3 vlan 4325
```

### Related Commands

Command	Description
<b>ping</b>	Sends an echo request packet to an address, and then awaits a reply to determine whether a device can be reached or is functioning.

# port0

To connect port0 to the local node of the Ethernet ring, use the **port0** command in Ethernet ring configuration mode. To disconnect the port, use the **no** form of this command.

**port0 interface** *type number*  
**no port0**

## Syntax Description

<b>interface</b> <i>type number</i>	Interface type and number. Enter the <b>interface</b> keyword followed by the interface type and interface number.
-------------------------------------	--

## Command Default

Port0 is not connected to the local node of the Ethernet ring.

## 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.

## Usage Guidelines

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

## Examples

The following is an example of the **port0** command used in an Ethernet ring configuration.

```
Device> enable
Device# configure terminal
Device(config)# ethernet ring g8032 ring1
Device(config-erp-ring)# port0 interface fastethernet 0/0/0
Device(config-erp-ring-port)#
```

## port0 service instance

To specify an Ethernet service instance for ring port0, use the **port0 service** command in Ethernet ring instance aps-channel configuration mode. To change the specification, use the **no** form of this command.

**port0 service instance** *instance-id*

**no port0 service instance** *instance-id*

### Syntax Description

<i>instance-id</i>	Instance identifier. Valid entries are in the range of 1 to 4000.
--------------------	---

### Command Default

An Ethernet service interface for ring port0 is not specified.

### 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.

### Examples

The following is an example of the **port0 service instance** 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)# port0 service instance 2
```

# port1

To connect port1 to the local node of the Ethernet ring, use the **port1** command in Ethernet ring configuration mode. To disconnect the port, use the **no** form of this command.

**port1** {*interface type number* | **none**}  
**no port1**

## Syntax Description

<b>interface</b> <i>type number</i>	Interface type and number. Enter the <b>interface</b> keyword followed by the interface type and interface number.
<b>none</b>	Indicates that the ring port is an open ring.

## Command Default

Port1 is not connected to the local node of the Ethernet ring.

## 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.

## Usage Guidelines

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

## Examples

The following is an example of the **port1** 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 g1
Device(config-erp-ring)# port1 interface fastethernet 0/0/0
Device(config-erp-ring-port)#
```

## port1 service instance

To specify an Ethernet service instance for ring port1, use the **port1** command in Ethernet ring instance aps-channel configuration mode. To change the specification, use the **no** form of this command.

**port1 service instance** {*instance-id* | **none**}

**no port1**

### Syntax Description

<i>instance-id</i>	Service instance identifier. Valid entries are in the range of 1 to 4000.
<b>none</b>	Indicates that the ring port is an open ring.

### Command Default

An Ethernet service instance for ring port1 is not specified.

### 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.

### Examples

The following is an example of the **port1 service instance** 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)# port1 service instance 2
```

## port-channel load-balance

To set the load distribution method among the ports in a bundle, use the **port-channel load-balance** command in global configuration mode. To reset the load distribution to the default settings, use the **no** form of this command.

**port-channel load-balance** *method* **module** *slot*

**no port-channel load-balance**

### Syntax Description

<i>method</i>	Load distribution method; see the “Usage Guidelines” section for a list of valid values.
<b>module</b>	Specifies the module on which the load-distribution method is set. This keyword is supported only on DFC systems.
<i>slot</i>	Number of the slot in the module.

### Command Default

The default **method** is **src-dst-ip**.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified to support the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	<p>This command was modified. The following keywords were added:  <b>dst-mixed-ip-port</b>, <b>src-dst-mixed-ip-port</b>, <b>src-mixed-ip-port</b>, and <b>exclude vlan</b>.</p> <ul style="list-style-type: none"> <li>• These keywords are supported on systems that are in PFC3C or PFC3CXL mode (PFC3C or PFC3CXL with no DFC3A or DFC3B/BXL) only.</li> <li>• The <b>exclude vlan</b> keyword is added only for IP-related load balance options.</li> </ul>



Release	Modification
12.2(50)SY	<p>This command was modified. The following methods were added:</p> <ul style="list-style-type: none"> <li>• <b>vlan-dst-ip</b></li> <li>• <b>vlan-dst-mixed-ip-port</b></li> <li>• <b>vlan-src-dst-ip</b></li> <li>• <b>vlan-src-dst-mixed-ip-port</b></li> <li>• <b>vlan-src-ip</b></li> <li>• <b>vlan-src-mixed-ip-port</b></li> </ul> <p>These methods are supported only in Cisco IOS Release 12.2(50)SY.</p>
15.1(2)SNG	<p>This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.</p>

## Usage Guidelines

Valid *method* values are as follows:

- **dst-ip** --Loads distribution on the destination IP address. Option to exclude VLAN in the distribution is provided using the **exclude vlan** keyword along with this method.
- **dst-mac** --Loads distribution on the destination MAC address.
- **dst-mixed-ip-port** --Loads distribution on the destination IP address and TCP or User Datagram Protocol (UDP) port. Option to exclude VLAN in the distribution is provided using the **exclude vlan** keyword along with this method.
- **dst-port** --Loads distribution on the destination port.
- **src-dst-ip** --Loads distribution on the source transfer or XOR-destination IP address. Option to exclude VLAN in the distribution is provided using the **exclude vlan** keyword along with this method.
- **src-dst-mac** --Loads distribution on the source XOR-destination MAC address.
- **src-dst-mixed-ip-port** --Loads distribution on the source XOR-destination IP address and the TCP or UDP port. Option to exclude VLAN in the distribution is provided using the **exclude vlan** keyword along with this method.
- **src-dst-port** --Loads distribution on the source XOR-destination port.
- **src-ip** --Loads distribution on the source IP address. Option to exclude VLAN in the distribution is provided using the **exclude vlan** keyword along with this method.
- **src-mac** --Loads distribution on the source MAC address.
- **src-mixed-ip-port** --Loads distribution on the source IP address and the TCP or UDP port. Option to exclude VLAN in the distribution is provided using the **exclude vlan** keyword along with this method.
- **src-port** --Loads distribution on the source port.
- **vlan-dst-ip** --VLAN, Dst IP Address
- **vlan-dst-mixed-ip-port** --VLAN, Dst IP Address, and TCP/UDP Port

- **vlan-src-dst-ip**--VLAN, Src XOR, Dst IP Address
- **vlan-src-dst-mixed-ip-port**--VLAN, Src XOR Dst IP Address, and TCP/UDP Port
- **vlan-src-ip**--VLAN, Src IP Address
- **vlan-src-mixed-ip-port**--VLAN, Src IP Address, and TCP/UDP Port

The **port-channel load-balance method module slot** command is supported on DFC systems only.

The **port-channel per-module load-balance** command allows you to enable or disable port-channel load-balancing on a per-module basis. You can enter the **port-channel load-balance method module slot** command to specify the load-balancing method on a specific module after you have entered the **port-channel per-module load-balance** command.

The following keywords are supported on systems that are in PFC3C or PFC3CXL mode (PFC3C or PFC3CXL with no DFC3A or DFC3B/BXL) only:

- **dst-mixed-ip-port**
- **src-dst-mixed-ip-port**
- **src-mixed-ip-port**



#### Note

If you change the load-balancing method, EtherChannel ports on DFC-equipped switching modules or an active supervisor engine in a dual supervisor engine configuration will flap.

## Examples

The following example shows how to set the load-distribution method to **dst-ip**:

```
Device(config)#
port-channel load-balance dst-ip
```

The following example shows how to set the load-distribution method on a specific module:

```
Device(config)#
port-channel load-balance dst-ip module 2
```

The following example shows how to set the load-distribution method excluding the VLAN option:

```
Device(config)#
port-channel load-balance dst-ip exclude vlan
```

## Related Commands

Command	Description
<b>interface port-channel</b>	Creates a port-channel virtual interface and enters interface configuration mode.
<b>port-channel load-balance mpls</b>	Sets the load distribution method among the ports in the bundle for MPLS packets.
<b>show etherchannel</b>	Displays the EtherChannel information for a channel.

## port-channel load-balance (interface)

To configure a member link for load balancing, a default service instance weight, or weighted load balancing on port-channel member links, use the **port-channel load-balance** command in interface configuration mode. To cause the default weight to revert to 1 and to disable weighted load balancing, use the **no** form of this command.

**port-channel load-balance** {**link** *link-id*| **weighted** {**default weight** *weight*| **link** {**all**| *link-id*}| **rebalance** {**disable**| *weight*} }

**no port-channel load-balance** {**link** *link-id*| **weighted** {**default weight**| **link** **rebalance**} }

### Syntax Description

<b>link</b>	Configures a member link for egress load balancing.
<i>link-id</i>	Integer from 1 to 16 that identifies the member link. <ul style="list-style-type: none"> <li>When used with the <b>weighted</b> keyword, the <i>link-id</i> is a comma-delimited list of member link IDs to use for weighted load balancing.</li> </ul>
<b>weighted</b>	Configures weighted load balancing on the port channel.
<b>default weight</b>	Configures a default weight for a service instance.
<i>weight</i>	Integer from 1 to 10000 that is the weight value. The default is 1. <ul style="list-style-type: none"> <li>When used with the <b>rebalance</b> keyword, this value is the threshold weight used to trigger automatic rebalancing. The default is 4.</li> </ul>
<b>all</b>	Configures load balancing across all active member links.
<b>rebalance</b>	Sets or disables the automatic rebalance threshold.
<b>disable</b>	Disables automatic rebalancing.

### Command Default

Service instance weight and weighted load balancing are not configured.

### Command Modes

Interface configuration (config-if)

**Command History**

Release	Modification
15.0(1)S	This command was introduced.

**Usage Guidelines**

When weighted load balancing enabled, the weight configured using this command is inherited by all service instances on the port channel that have not been specifically configured with a weight.

Configuring a default weight is optional; the default weight value is 1.

Use of the **weighted** and **link** keywords is required to enable weighted load balancing on a port channel. When the **all** keyword is configured, traffic is distributed across all active member links in the port channel. When one or more member links is specified, traffic is distributed across only those member links. To allow for out-of-order configuration, link IDs not yet assigned to member links may be specified. Issuing this command with the **weighted** and **link** keywords more than once under the same port-channel interface results in overwriting the command settings previously configured.

If this command is configured with a list of link IDs and the member link corresponding to one of those link IDs is later configured with a different ID, a warning is displayed on the console that notifies the user that the action will affect the current load-balancing activity.

When the **disable** keyword is configured, automatic rebalancing is not performed and the operator must manually invoke rebalancing by issuing the **port-channel load-balance weighted rebalance** command in privileged EXEC mode.

When the **disable** keyword is not configured, either the configured or a default weight is used to automatically rebalance service instances. Automatic rebalancing occurs when the average absolute deviation (AAD) of the current distribution exceeds the configured threshold and when the resulting AAD of the rebalanced distribution is less than the current AAD. If automatic rebalancing does not result in a lower AAD, the rebalancing is not done, even if the current AAD exceeds the threshold.

The AAD calculation is  $(1/n) * \sum(|w(i) - m|)$  for all  $n$  member links where:

$n$  = number of member links

$m$  = mean of member link weights (sum of all Ethernet service instance weights divided by  $n$ )

$w(i)$  = sum of Ethernet service instance weights on member link  $i$

Two conditions cause the **port-channel load-balance** command to fail:

- An invalid weight is configured.
- An invalid link ID is provided.

**Examples**

The following example shows how to configure port-channel load balancing for all port-channel member links:

```
Router(config)# interface port-channel1
Router(config-if)# port-channel load-balance weighted link all
```

## port-channel load-balance mpls

To set the load-distribution method among the ports in the bundle for Multiprotocol Label Switching (MPLS) packets, use the **port-channel load-balance mpls** command in global configuration mode. To reset the load distribution to the default settings, use the **no** form of this command.

**port-channel load-balance mpls** {label| label-ip}

**no port-channel load-balance mpls**

### Syntax Description

<b>label</b>	Specifies using the MPLS label to distribute packets; see the “Usage Guidelines” section for additional information.
<b>label-ip</b>	Specifies using the MPLS label or the IP address to distribute packets; see the “Usage Guidelines” section for additional information.

### Command Default

label-ip

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(14)SX	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.

### Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you select **label**, these guidelines apply:

- With only one MPLS label, the last MPLS label is used.
- With two or more MPLS labels, the last two labels (up to the fifth label) are used.

If you select **label-ip**, these guidelines apply:

- With IPv4 and three or fewer labels, the source IP address XOR-destination IP address is used to distribute packets.
- With four or more labels, the last two labels (up to the fifth label) are used.

- With non-IPv4 packets, the distribution method is the same as the **label** method.

## Examples

This example shows how to set the load-distribution method to **label-ip**:

```
Router(config)#  
port-channel load-balance mpls label-ip  
Router(config)#
```

## Related Commands

Command	Description
<b>interface port-channel</b>	Creates a port-channel virtual interface and enters interface configuration mode.
<b>show etherchannel</b>	Displays the EtherChannel information for a channel.

# port-channel load-balance weighted rebalance

To perform a rebalancing of all port-channel interfaces configured with weighted load balancing, use the **port-channel load-balance weighted rebalance** command in privileged EXEC mode.

**port-channel load-balance weighted rebalance** [**interface port-channel** *number*]

## Syntax Description

<b>interface</b>	(Optional) Specifies a port channel enabled for weighted load balancing.
<b>port-channel</b>	(Optional) Specifies an Ethernet channel of interfaces.
<i>number</i>	(Optional) Integer from 1 to 564 that identifies the port-channel interface.

## Command Default

Load rebalancing is not performed.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.0(1)S	This command was introduced.

## Usage Guidelines

If a port-channel interface is specified, only that interface is rebalanced; otherwise all port channels with weighted load balancing enabled are rebalanced.

This command may be used when automatic rebalancing is disabled via the **port-channel load-balance weighted rebalance disable** command or when a rebalancing of service instances is desired prior to reaching the automatic rebalance threshold.

If the specified interface is not a port channel enabled for weighted load balancing, the **port-channel load-balance weighted rebalance** command has no effect on load balancing on that interface.

## Examples

The following example shows how to force a rebalancing of service instances, based on their assigned weights, for all port channels with weighted load balancing enabled:

```
Router# port-channel load-balance weighted rebalance
```

**Related Commands**

Command	Description
<b>port-channel load-balance (interface)</b>	Configures a member link for load balancing, a default service instance weight, or weighted load balancing on port-channel member links.



# priority1

To set a preference level for a Precision Time Protocol clock, use the **priority1** command in PTP clock configuration mode. To remove a priority1 configuration, use the **no** form of this command.

**priority1** *priorityvalue*

**no priority1** *priorityvalue*

## Syntax Description

<i>priorityvalue</i>	Number value of the preference level. The range is from 0 to 255; lower values indicate a higher precedence. The default value is 128.
----------------------	--

## Command Default

The default preference level is 128.

## Command Modes

PTP clock configuration (config-ptp-clk)

## Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

Slave devices use the priority1 value when selecting a master clock. The priority1 value has precedence over the priority2 value.

## Examples

The following example shows how to configure a ptp priority1 value:

```
Device> enable
Device# configure terminal
Device# ptp clock ordinary domain 0
Device(config-ptp-clk)# priority1 128
Device(config-ptp-clk)# end
```

## Related Commands

Command	Description
<b>priority2</b>	Sets the PTP priority2 value.

# priority2

To set a secondary preference level for a Precision Time Protocol clock, use the **priority2** command in PTP clock configuration mode. To remove a priority2 configuration, use the **no** form of this command.

**priority2** *priorityvalue*

**no priority2** *priorityvalue*

## Syntax Description

<i>priorityvalue</i>	The number value of the preference level. The range is from 0 to 255; lower values indicate a higher precedence. The default value is 128.
----------------------	--

## Command Default

The default preference level is 128.

## Command Modes

PTP clock configuration (config-ptp-clk)

## Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

Slave devices use the priority2 value to select a master clock; the priority2 value is only considered when the device cannot use priority1 and other clock attributes to select a clock.

## Examples

The following example shows how to configure the ptp priority2 value:

```
Device> enable
Device# configure terminal
Device# ptp clock ordinary domain 0
Device(config-ptp-clk)# priority2 128
Device(config-ptp-clk)# end
```

## Related Commands

Command	Description
<b>priority1</b>	Sets the PTP priority1 value.

# profile

To associate an Ethernet ring profile with an instance, use the **profile** command in Ethernet ring instance configuration mode. To remove the association, use the **no** form of this command.

**profile** *profile-name*

**no profile**

## Syntax Description

<i>profile-name</i>	Ethernet profile name. The profile name can be a maximum of 32 alphanumeric characters.
---------------------	---

## Command Default

An Ethernet ring profile is not associated with an instance.

## 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.

## Usage Guidelines

Associating an Ethernet ring profile with an instance is optional. The Ethernet ring profile is owned by the Ethernet Ring Protection (ERP) controller.

## Examples

The following is an example of the **profile** 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)# profile profile1
```

## pseudowire (Layer 2)

To define the maximum and watermark limits for pseudowires from a peer provider edge (PE) device, use the **pseudowire** command in Layer 2 (L2) subscriber group command mode. To disable the maximum and watermark limits, use the **no** form of this command.

**pseudowire** {**maximum**|**watermark high**} *limit*

**no pseudowire** {**maximum**|**watermark high**}

### Syntax Description

<b>maximum</b>	Specifies the maximum number of Any Transport over MPLS (AToM) virtual circuits (VCs) allowed to be configured from the peer PE devices.
<b>watermark high</b>	Specifies the high watermark limit for the AToM VCs from the peer PE devices.
<i>limit</i>	High watermark value. Valid values are from 1 to 16384.

### Command Default

The maximum and watermark limits for pseudowires from the peer PE devices is not configured.

### Command Modes

L2 subscriber group configuration (config-l2-sub-gr)

### Command History

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

### Usage Guidelines

If the number of AToM VCs exceed the maximum and watermark limits for the pseudowire, syslog messages are displayed.

### Examples

The following example shows how to configure the maximum number of AToM VCs on a pseudowire:

```
Router# configure terminal
Router(config)# 12 subscriber authorization group group1
Router(config-l2-sub-gr)# pseudowire maximum 58
```

**Related Commands**

Command	Description
<b>l2 subscriber</b>	Creates an L2 subscriber authorization group, and enters L2 subscriber group mode.
<b>peer</b>	Defines the target LDP peer PE information.
<b>service-policy type control (Layer 2)</b>	Attaches an ISG control service policy to an L2 subscriber authorization group.

# ptp clock

To create a Precision Time Protocol (PTP) clock and specify the clock mode, use the **ptp clock** command in the global configuration mode. To remove a PTP clock configuration, use the **no** form of this command.

**ptp clock** {**ordinary**| **transparent**} **boundary domain** *domain*

**no ptp clock** {**ordinary**| **transparent**} **boundary domain** *domain*

## Syntax Description

<b>ordinary</b>	Sets the PTP clock to ordinary clocking mode.
<b>transparent</b>	Sets the PTP clock to transparent clock mode; the router modifies outgoing PTP sync and delay-request messages to account for residence time using the correction field in the follow-up message.
<b>boundary</b>	Sets the PTP clock to boundary clock mode; the router participates in selecting the best master clock and can act as the master clock if no better clocks are detected.
<i>domain</i>	The PTP clocking domain number. Valid values are from 0 to 127.

## Command Default

A PTP clock is not created and the clock mode is not specified.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

This command creates a new PTP clock and enters clock configuration mode.

## Examples

The following example shows how to configure a PTP clock and enter clock configuration mode:

```
Device> enable
Device# configure terminal
```

```
Device(config)# ptp clock ordinary domain 0  
Device(config-ptp-clk)#
```

**Related Commands**

Command	Description
<b>clock-port</b>	Specifies the mode of a PTP clock port.

## rewrite egress tag

To perform an encapsulation adjustment on a frame egressing a service instance, use the **rewrite egress tag** command in service instance configuration mode. To delete an encapsulation adjustment, use the **no** form of this command.

**rewrite egress tag** {**pop** {**1** | **2**} | **push** {**dot1ad** *vlan-id* [**dot1q** *vlan-id*] | **dot1q** *vlan-id* [**second-dot1q** *vlan-id*] | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} [**second-dot1q** *vlan-id*]]} | **translate** {**1-to-1** {**dot1ad** *vlan-id* | **dot1q** *vlan-id* [**vlan-type** {**0x88a8** | **0x9100** | **0x9200**}]} | **1-to-2** {**dot1ad** *vlan-id* | **dot1q** *vlan-id* | **dot1q** *vlan-id* [**second-dot1q** *vlan-id*] | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} **second-dot1q** *vlan-id*} | **2-to-1** {**dot1ad** *vlan-id* | **dot1q** *vlan-id* [**vlan-type** {**0x88a8** | **0x9100** | **0x9200**}]} | **2-to-2** {**dot1ad** *vlan-id* | **dot1q** *vlan-id* [**second-dot1q** *vlan-id*] | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} **second-dot1q** *vlan-id*}}

**no rewrite egress**

### Syntax Description

<b>pop</b>	Specifies removing a tag.
<b>1</b>	Specifies the outermost tag in a packet.
<b>2</b>	Specifies the two outermost tags in a packet.
<b>push</b>	Adds a tag.
<b>dot1ad</b>	Specifies a dot1ad VLAN tag.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies a VLAN.
<b>dot1q</b>	Specifies a tag with the dot1q Ethertype.
<b>second-dot1q</b>	Specifies a second tag with the dot1q Ethertype.
<b>vlan-type</b>	Specifies type of VLAN protocol.
<b>0x88a8</b>	Specifies VLAN protocol type.
<b>0x9100</b>	Specifies VLAN protocol type.
<b>0x9200</b>	Specifies VLAN protocol type.
<b>translate</b>	Translates a VLAN tag.
<b>1-to-1</b>	Translates a VLAN tag to a different VLAN tag.
<b>1-to-2</b>	Translates a single VLAN tag to two different VLAN tags.
<b>2-to-1</b>	Translates two different VLAN tags to a single VLAN tag.



<b>2-to-2</b>	Translates two VLAN tags to two different VLAN tags.
---------------	--

**Command Default** The frame is left intact on egress.

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2S	This command was introduced.

**Usage Guidelines** Use the **rewrite egress tag** command to modify packet VLAN tags. You can use this command to emulate traditional 802.1Q tagging and to facilitate VLAN translation and IEEE 802.1QinQ (QinQ) encapsulation. An encapsulation method must be configured before you can use the **rewrite egress tag** command.

**Examples** The following example shows how to specify the encapsulation adjustment that is needed on the ingress frame to the service instance:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 2/0/0
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite egress tag push dot1q 200
```

## rewrite ingress tag

To specify the encapsulation adjustment to be performed on a frame ingressing a service instance, use the **rewrite ingress tag** command in Ethernet service configuration mode. To delete the encapsulation adjustment, use the **no** form of this command.

```
rewrite ingress tag {pop | {1 | 2} [symmetric]} push {dot1ad vlan-id [dot1q vlan-id] [symmetric] | dot1q
vlan-id [second-dot1q vlan-id] [symmetric]} | translate {1-to-1 {dot1ad vlan-id dot1q vlan-id}
[symmetric]} | 1-to-2 {dot1ad vlan-id dot1q vlan-id} | dot1q vlan-id second-dot1q vlan-id [symmetric] |
2-to-1 {dot1ad vlan-id dot1q vlan-id [symmetric]} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id
[symmetric]}
```

**no rewrite ingress tag**

### Syntax on the Cisco ASR 1000 Series Aggregation Router

#### Syntax Description

**rewrite ingress tag** {pop {1 | 2} [symmetric] | push {dot1ad vlan-id [dot1q vlan-id] [symmetric] | dot1q vlan-id [second-dot1q vlan-id] [symmetric] | vlan-type {0x88a8 | 0x9100 | 0x9200} [second-dot1q vlan-id] [symmetric]} | translate {1-to-1 {dot1ad vlan-id dot1q vlan-id [vlan-type {0x88a8 | 0x9100 | 0x9200}] [symmetric]} | 1-to-2 {dot1ad vlan-id dot1q vlan-id dot1q vlan-id [second-dot1q vlan-id] [vlan-type {0x88a8 | 0x9100 | 0x9200}] second-dot1q vlan-id} [symmetric] | 2-to-1 {dot1ad vlan-id [symmetric] | dot1q vlan-id [vlan-type {0x88a8 | 0x9100 | 0x9200}] [symmetric]} | 2-to-2 {dot1ad vlan-id dot1q vlan-id [symmetric] | dot1q vlan-id [second-dot1q vlan-id] [vlan-type {0x88a8 | 0x9100 | 0x9200}] second-dot1q vlan-id} [symmetric]}}

**no rewrite ingress tag**

<b>pop</b>	Removes a tag from a packet.
<b>{1   2}</b>	Specifies either the outermost tag or the two outermost tags for removal from a packet.
<b>symmetric</b>	(Optional) Indicates a reciprocal adjustment to be done in the egress direction. For example, if the ingress pops a tag, the egress pushes a tag and if the ingress pushes a tag, the egress pops a tag.
<b>push</b>	Adds a tag.
<b>dot1ad</b>	Specifies an IEEE 802.1ad tag.
<i>vlan-id</i>	Integer in the range 1 to 4094 that identifies the VLAN.
<b>dot1q</b>	Specifies an IEEE 802.1Q tag.
<b>second-dot1q</b>	Specifies a different 802.1Q tag at the ingress service instance.

<b>vlan-type</b>	Specifies the type of VLAN protocol.
<b>0x88a8</b>	Specifies the protocol type 0x88a8.
<b>0x9100</b>	Specifies the protocol type 0x9100.
<b>0x9200</b>	Specifies the protocol type 0x9200.
<b>translate</b>	Translates, by VLAN ID, a tag or a pair of tags defined in the <b>encapsulation</b> command.
<b>1-to-1</b>	Translates a single tag defined by the <b>encapsulation</b> command to a single tag defined in the <b>rewrite ingress tag</b> command.
<b>1-to-2</b>	Translates a single tag defined by the <b>encapsulation</b> command to a pair of tags defined in the <b>rewrite ingress tag</b> command.
<b>2-to-1</b>	Translates, by VLAN ID, a pair of tags defined by the <b>encapsulation</b> command to a single tag defined in the <b>rewrite ingress tag</b> command.
<b>2-to-2</b>	Translates, by VLAN ID, a pair of tags defined by the <b>encapsulation</b> command to a pair of tags defined in the <b>rewrite ingress tag</b> command.

**Command Default**

The frame is left intact on ingress (the service instance is equivalent to a trunk port).

**Command Modes**

Ethernet service (config-if-srv)

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
Cisco IOS XE Release 3.5S	This command was implemented on the Cisco ASR 903 Router.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

The **symmetric** keyword is accepted for all rewrite operations only when a single VLAN is configured in encapsulation. If a list of VLANs or a range of VLANs is configured in encapsulation, the **symmetric** keyword is accepted only for push rewrite operations.

The **pop** keyword assumes the elements being popped are defined by the encapsulation type. The exception case should be drop the packet.

The **translate** keyword assumes the tags being translated from are defined by the encapsulation type. In the 2-to-1 option, the “2” means 2 tags of a type defined by the **encapsulation** command. The translation operation requires at least one “from” tag in the original packet. If the original packet contains more tags than the ones defined in the “from,” the operation should be done beginning on the outer tag. Exception cases should be dropped.

### Examples

The following example shows how to specify the encapsulation adjustment to be performed on the frame ingressing the service instance:

```
Device> enable
Device# configure terminal
Device(config) interface gigabitethernet 2/0/0
Device(config-if) # service instance 100 ethernet
Device(config-if-srv) # encapsulation dot1q 100
Device(config-if-srv) # rewrite ingress tag push dot1q 200
```

### Related Commands

Command	Description
<b>encapsulation</b>	Sets the encapsulation method used by an interface.

# rpl

To specify one ring port on the local node as the Ring Protection Link (RPL) owner, neighbor, or next neighbor, use the **rpl** command in Ethernet ring instance configuration mode. To remove the specification for the port as the RPL owner, neighbor, or next neighbor, use the **no** form of this command.

**rpl** {port0| port1} {owner| neighbor| next-neighbor}

**no rpl**

## Syntax Description

<b>port0</b>	Specifies port0 as the ring port.
<b>port1</b>	Specifies port1 as the ring port.
<b>owner</b>	Specifies the ring port as the RPL owner.
<b>neighbor</b>	Specifies the ring port as the RPL neighbor.
<b>next-neighbor</b>	Specifies the ring port as the RPL next neighbor.

## Command Default

A ring port is not specified as the RPL owner, neighbor, or next neighbor.

## 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.

## Usage Guidelines

Only one port (either port0 or port1) can be specified as the RPL owner, neighbor, or next neighbor.

## Examples

The following is an example of the **rpl** 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)# rpl port0 neighbor
```

# sender-id

To indicate the contents of the Sender ID TLV field transmitted in Ethernet connectivity fault management (CFM) messages for members of a maintenance domain, use the **sender-id** command in Ethernet CFM configuration mode. To send no sender ID information, use the **no** form of this command.

- sender-id chassis
- no sender-id chassis

## Syntax Description

chassis	Sends only the chassis ID information.
---------	--

## Command Default

The Sender ID TLV is not included in messages.

## Command Modes

Ethernet CFM configuration (config-ecfm)

## 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.

## Usage Guidelines

This command has lower precedence than the **sender-id** command issued at the maintenance association. To override the configuration at the maintenance association, configure the service ID as “none.”

## Examples

The following example shows how to include only the chassis ID information in the Sender ID TLV:

```
Device(config)# ethernet cfm domain customerA level 5
Device(config-ecfm)# sender-id chassis
```

## sender-id (CFM-srv)

To indicate the contents of the Sender ID TLV field transmitted in Ethernet connectivity fault management (CFM) messages for the maintenance association, use the **sender-id** command in Ethernet CFM service configuration mode. To send no sender ID information, use the **no** form of this command.

**sender-id** {chassis| none}

**no sender-id** {chassis| none}

### Syntax Description

<b>chassis</b>	Sends only the chassis ID information.
<b>none</b>	No sender ID information is sent.

### Command Default

The Sender ID TLV is not included in messages.

### Command Modes

Ethernet CFM service configuration (config-ecfm-srv)

### 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

This command has higher precedence than the **sender-id** command issued for the maintenance domain. The default is that the enclosing maintenance domain determines the Sender ID.

### Examples

The following example shows how to include only the chassis ID information in the Sender ID TLV:

```
Device(config)# ethernet cfm domain customerA level 5
Device(config-ecfm)# service vlan-id 17 port
Device(config-ecfm-srv)# sender-id chassis
```

## service (CFM-srv)

To configure a maintenance association within a maintenance domain and enter Ethernet connectivity fault management (CFM) service configuration mode (config-ecfm-srv), use the **service** command in Ethernet CFM configuration mode. To remove the configuration, use the **no** form of this command.

**service** {*ma-name*| *ma-num*} **vlan-id** *vlan-id* **vpn-id** *vpn-id* [**port** **vlan** *vlan-id* [**direction down**]]

**no service** {*ma-name*| *ma-num*} **vlan-id** *vlan-id* **vpn-id** *vpn-id* [**port** **vlan** *vlan-id* [**direction down**]]

### Syntax Description

<i>ma-name</i>	Short maintenance association name.
<i>ma-num</i>	Integer from 0 to 65535 that identifies the maintenance association.
<b>vlan-id</b>	Configures a primary VLAN.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the primary VLAN.
<b>vpn-id</b>	Configures a virtual private network (VPN).
<i>vpn-id</i>	Integer from 1 to 32767 that identifies the VPN.
<b>port</b>	(Optional) Configures a DOWN service direction without a VLAN association.
<b>vlan</b>	(Optional) Configures a VLAN.
<b>direction</b>	(Optional) Configures the service direction. The default is "up."
<b>down</b>	(Optional) Configures the direction toward the LAN.

### Command Default

No maintenance associations are configured.

### Command Modes

Ethernet CFM configuration (config-ecfm)

### 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.



### Usage Guidelines

The maintenance association ID (MAID) is a combination of a maintenance domain ID and the short maintenance association name, and the length of the MAID TLV should not exceed 48 characters.

If you configure the same short maintenance association name for two VLANs in the same domain, an error message is displayed and the command is rejected.

If you specify the service direction as down (outward to the LAN), you can create multiple outward services at the same level containing an overlapping set of VLANs. The set of VLANs in an outward service can also overlap with inward services. A set of VLANs between inward services at the same level must be unique.

### Examples

The following example shows how to configure a maintenance association with the ID 10, VLAN 17, and service direction toward the LAN within the customerA maintenance domain:

```
Device(config)# ethernet cfm domain customerA level 5
Device(config-ecfm)# service 10 vlan-id 17 direction down
Device(config-ecfm-srv)#
```

## service evc

To set a universally unique ID for a customer service instance (CSI) within a maintenance domain, use the **service evc** command in Ethernet CFM configuration mode. To remove a universally unique ID for a service within a maintenance domain, use the **no** form of this command.

**service** *csi-id* **evc** *evc-name* **vlan** *vlan-id* **direction** **down**

**no service** *csi-id* **evc** *evc-name* **vlan** *vlan-id* **direction** **down**

### Syntax Description

<b>service</b>	Specifies the service instance.
<i>csi-id</i>	String of a maximum of 100 characters that identifies the CSI.
<b>evc</b>	Specifies the Ethernet virtual circuit (EVC).
<i>evc-name</i>	String that identifies the Ethernet virtual circuit (EVC).
<b>vlan</b>	Specifies the VLAN.
<i>vlan-id</i>	String the VLAN ID. Range is from 1 to 4094.
<b>direction</b>	Specifies the service direction.
<b>down</b>	Specifies the direction towards the LAN.

### Command Default

No universally unique ID is set for the CSI.

### Command Modes

Ethernet CFM configuration (config-ether-cfm)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

## Usage Guidelines

A fully qualified service ID consists of a service ID plus a domain name. Service IDs identify customers within a domain. Ethernet connectivity fault management (CFM) requires that service IDs are unique in a network.

You must configure a service EVC before you can configure a maintenance endpoint (MEP) for a domain.

The following restrictions apply when you issue the **service evc** command:

- Maintenance domains on the same device cannot have the same name.
- Two domains at the same maintenance level cannot be on the same EVC unless one or both of the domains are outward domains.
- A service ID must be unique within a single maintenance domain.

For two domains at the same maintenance level, the same service ID can be used for two different EVCs. If you try to configure the same service ID for two EVCs in the same domain, the command is rejected and an error message is displayed.

Specifying a domain as outward allows you to create multiple outward domains at the same level with a set of services that overlap. These EVCs can also overlap with inward domains. Note that a set of EVCs overlapping inward domains at only the same level must be unique.

You can use the same service ID in the same EVC or different EVCs if the service IDs are in different levels.

Before you remove a service ID, all MEPs corresponding to the service must be removed.

On Cisco 7600 series routers, a VLAN service and an EVC service may have the same service ID if the bridge domain is associated with an EVC and the bridge-domain ID equals the VLAN service ID. This situation occurs because the bridge domain and the VLAN of the same number form a single broadcast domain representing the same CFM service.

## Examples

The following example shows how to configure an Ethernet CFM service with EVC evc100:

```
ethernet cfm domain PROVIDER level 4
 service provider_100 evc evc100
```

The following example shows how to configure Ethernet CFM service on a Cisco Route Switch Processor 720. You must configure the VLAN and EVC services with the same name because VLAN 100 and bridge domain 100, which is associated with EVC 100, represent a single broadcast domain.

```
ethernet cfm domain CUSTOMER level 7
 service customer_100 vlan 100
 service customer_100 evc evc100
!
ethernet evc evc100
!
interface Ethernet0/0
 service instance 100 ethernet evc100
 encapsulation dot1q 100
 bridge-domain 100
```

## Related Commands

Command	Description
<b>service vlan</b>	Sets a unique service ID within a maintenance domain.



## service icc

To set the ITU-T Y.1731 Carrier Code (ICC)-based maintenance entity group (MEG) identifier within a maintenance domain, use the **service icc** command in Ethernet CFM configuration mode. To remove the ICC-based MEG identifier, use the **no** form of this command.

**service icc** *icc-code meg-code* {**evc** *evc-name* | [**direction down** | **vlan**]} [**port** | **vlan** *vlan-id* **inner-vlan** *inner-vlan-id*]

**no service icc** *icc-code meg-code* {**evc** *evc-name* | [**direction down** | **vlan**]} [**port** | **vlan** *vlan-id* **inner-vlan** *inner-vlan-id*]

### Syntax Description

<i>icc-code</i>	String from 1 to 6 characters that identifies the ITU carrier code.
<i>meg-code</i>	String from 1 to 12 characters that identifies the unique MEG code.
<b>evc</b>	Specifies the Ethernet virtual circuit (EVC).
<i>evc-name</i>	String from 1 to 100 characters that identifies the EVC.
<b>direction down</b>	(Optional) Configures a DOWN service direction.
<b>vlan</b>	(Optional) Configures a primary VLAN.
<b>port</b>	Configures a DOWN service direction without a VLAN association.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the primary VLAN.
<b>inner-vlan</b>	Specifies the inner VLAN.
<i>inner-vlan-id</i>	Integer from 1 to 4094 that identifies the inner VLAN.

### Command Default

The ICC-based MEG code is not set.

### Command Modes

Ethernet CFM configuration (config-ecfm)

### Command History

Release	Modification
15.2(1)S	This command was introduced.

Release	Modification
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

### Usage Guidelines

To enter the Ethernet CFM configuration mode, use the **ethernet cfm domain level** command.

The **service icc** command places the command-line interface (CLI) into Ethernet connectivity fault management (CFM) service configuration mode (config-ecfm-srv).

### Examples

In the following example, an ICC-based MEG code of icc1 has been configured.

```
Router(config)# ethernet cfm domain customerA level 5  
Router(config-ecfm)#service icc icc1 1234567890 evc evc5 direction down  
Router(config-ecfm-srv)#
```

### Related Commands

Command	Description
<b>ethernet cfm domain level</b>	Defines a CFM maintenance domain at a particular maintenance level and puts the CLI into Ethernet CFM configuration mode.

## service instance dynamic

To configure an Ethernet Layer 2 context service instance on an interface and to enter service instance configuration mode, use the **serviceinstance dynamic** command in interface configuration mode. To delete an Ethernet Layer 2 context service instance, use the **no** form of this command.

**service instance dynamic** *L2-id* **ethernet**

**no service instance** *id*

### Syntax Description

<i>L2-id</i>	Layer 2 context identifier. Valid values are from 1 to 4000.
<b>ethernet</b>	Configures an Ethernet instance.

### Command Default

Ethernet Layer 2 context service instances are not configured.

### Command Modes

Interface configuration (config-if)

### Command History

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

### Usage Guidelines

The **serviceinstance dynamic** command defines that a service instance is an Ethernet Layer2 context. This command works as a forwarder service for this service instance. If this command is configured, then you cannot configure any other forwarding services such as xconnect, bridge-domain and connect. This command configured on any platform indicates that the traffic classified on this service instance is not going to be dropped, instead the traffic will be punted to the First Sign of Life (FSOL) handling mechanism.

### Examples

The following example shows how to define an Ethernet Layer 2 service instance and enter service instance configuration mode:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service instance dynamic 100 ethernet
```

### Related Commands

Command	Description
<b>encapsulation dot1q</b>	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

Command	Description
<b>initiator</b>	Enables an initiator for detecting the FSOL under Ethernet Layer 2 context.



## service instance ethernet

To configure an Ethernet service instance on an interface, use the **service instance ethernet** command in interface configuration mode. To delete a service instance, use the **no** form of this command.

**service instance** [**trunk**] *id* **ethernet** [*evc-name*]

**no service instance** [**trunk**] *id* **ethernet**

### Cisco ASR 901 Series Aggregation Services Router

**service instance** *instance-id* **ethernet** [*evc-name*]

#### Syntax Description

<b>trunk</b>	(Optional) Indicates that the service instance will be configured on a trunk interface.
<i>id</i>	Integer that uniquely identifies a service instance on an interface. The value varies by the platform. Range: 1 to 4294967295. The identifier need not map to a VLAN and is local in scope to the interface.
<i>evc-name</i>	(Optional) String that associates an Ethernet virtual connection (EVC) to the service instance. Maximum: 100 bytes.
<i>instance-id</i>	Service instance number that identifies the Ethernet Flow Point (EFP). Range: 1 to 8000.

#### Command Default

No Ethernet service instances are defined.

#### 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.
12.2(33)SRE	This command was modified. The <b>group</b> command is now available after entering Ethernet service configuration mode.

Release	Modification
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S to provide support for the Cisco ASR 903 Router. This command was modified to include support for Ethernet Flow Points (EFPs) on trunk ports (interfaces). The optional <b>trunk</b> keyword was added.
Cisco IOS XE Release 3.7S	This command was modified. Support for short maintenance-association (MA) names in the MEP parser syntax was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

A service instance is a configuration object (container) that holds all management and control-plane attributes and parameters that apply to that service instance on a per-port basis. Different service instances that correspond to the same EVC must share the same name. Service instances are associated with a global EVC object through their shared name.

After you enter the **service instance ethernet** command, the device enters Ethernet service configuration mode, and these configuration commands are available:

- **default** —Sets the service instance to its default state.
- **ethernet lmi ce-vlan map** —Configures Ethernet Local Management Interface (Ethernet LMI) parameters. See the **ethernet lmi ce-vlan map** command.
- **exit** —Exits Ethernet service configuration mode and returns to global configuration mode.
- **no** —Negates a command or returns a command to its default setting.
- **group** (service group)—Allows a member to be added to a service group. The service group must already exist when the **group** command is issued.

In Cisco IOS XE Release 3.7S and later releases, configuring a local maintenance endpoint (MEP) on EFPs is rejected when there are multiple MAs mapping to the same service in the domain.

## Examples

The following example shows how to define an Ethernet service instance and enter Ethernet service configuration mode for an EVC:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/0
Device(config-if)# service instance 333 ethernet test
Device(config-if-srv)#
```

The following example shows how to configure a short MA name in the MEP parser syntax.

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/0
Device(config-if)# service instance 1 ethernet evc10
Device(config-srv)# encapsulation dot1q 10
Device(config-srv)# bridge-domain 10
Device(config-srv)# cfm mep domain level3 mpid 1 service MA1
```

The following example shows how to define an Ethernet service instance and enter Ethernet service configuration mode for an EVC on a Cisco ASR 901 Series Aggregation Services router:

```
Device> enable
Device# configure terminal
Device (config)# interface ethernet 0/0
Device (config-if)# service instance 22 ethernet evc3
Device (config-if-srv)#
```

#### Related Commands

Command	Description
<b>ethernet evc</b>	Defines an EVC and enters EVC configuration mode.
<b>ethernet lmi ce-vlan map</b>	Configures Ethernet Local Management Interface parameters.
<b>group (service group)</b>	Adds a member to a service group.
<b>show ethernet service instance</b>	Displays information about configured Ethernet service instances.

# service instance ethernet (mac-tunnel)

To define an Ethernet flow point (EFP) that corresponds to a specific service instance ID (I-SID) encapsulation and to place the command-line interface (CLI) into MAC tunnel service configuration mode, use the **service instance ethernet** command in MAC-in-MAC tunnel configuration mode. To delete an EFP, use the **no** form of this command.

**service instance** *id* **ethernet**  
**no service instance** *id*

## Syntax Description

<i>id</i>	Integer in the range of 1 to 16384 that identifies an EFP.
-----------	--

## Command Default

No EFPs are defined.

## Command Modes

MAC-in-MAC tunnel configuration (config-tunnel-minm)

## Command History

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

## Usage Guidelines

This command is required to do MAC-in-MAC tunneling.

The service instance ID is unique for all MAC tunnels; for example, if service instance 10 is configured under MAC tunnel 1, service instance 10 cannot be configured under any other MAC tunnel.

## Examples

The following example shows how to define an EFP and place the CLI into MAC tunnel service configuration mode:

```
Router(config)# ethernet mac-tunnel virtual 100
Router(config-tunnel-minm)# service instance 5 ethernet
Router(config-tunnel-srv)#
```

## service vlan

To set a universally unique ID for a customer service instance (CSI) within a maintenance domain, use the **service vlan** command in Ethernet connectivity fault management (CFM) configuration mode. To remove a universally unique ID for a service within a maintenance domain, use the **no** form of this command.

**service** *csi-id* **vlan** *vlan-id*

**no service** *csi-id* **vlan** *vlan-id*

### Syntax Description

<i>csi-id</i>	String of a maximum of 100 characters that identifies the CSI.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the VLAN.

### Command Default

No universally unique ID is set for the CSI.

### Command Modes

Ethernet CFM configuration (config-ether-cfm)

### 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.
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

A fully qualified service ID consists of a service ID plus a domain name. Service IDs identify customers within a domain. Ethernet CFM requires that service IDs are unique in a network.

You must configure a service VLAN before you can configure a MEP for a domain.

The following restrictions apply when you issue the **service vlan** command:

- Maintenance domains on the same device cannot have the same name.
- Two domains at the same maintenance level cannot be on the same VLAN unless one or both of the domains are outward domains.
- A service ID must be unique within a single maintenance domain.

For two domains at the same maintenance level, the same service ID can be used for two different VLANs. If you try to configure the same service ID for two VLANs in the same domain, the command is rejected and an error message displays.

Specifying a domain as outward allows you to create multiple outward domains at the same level with a set of services that overlap. These VLANs also can overlap with inward domains. Note that a set of VLANs overlapping inward domains at only the same level must be unique.

You can use the same service ID in the same VLAN or different VLANs if the service IDs are in different levels.

Before you remove a service ID, all MEPs corresponding to the service must be removed.

## Examples

The following example shows how to set a unique service ID within a maintenance domain:

```
Device(config-ether-cfm) # service firstinstance vlan 35
```

## service-policy type control policy

To attach an Intelligent Service Gateway (ISG) control service policy to a Layer 2 subscriber authorization group, use the **service-policy type control policy** command in Layer 2 subscriber group configuration mode. To remove the configuration, use the **no** form of this command.

**service-policy type control policy** *policy-name*

**no service-policy type control policy** *policy-name*

### Syntax Description

<i>policy-name</i>	Specifies the ISG control service-policy name.
--------------------	--

### Command Default

The global control policy is used.

### Command Modes

Layer 2 subscriber group configuration (config-l2-sub-gr)

### Command History

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

### Usage Guidelines

ISG control policies define the actions that are taken in response to specific events and conditions. You can configure an ISG control policy to control the behavior of the dynamically created Ethernet ISG sessions.

To define a control policy, you must define a control class map to identify events and conditions, and then define a control policy map to bind the control class map to different actions. You can define the control policy at the global level, interface level, or dynamic Ethernet session target level. If control policies are configured at multiple levels, the control policy at the inner level has higher precedence over those at levels above the inner level.

### Examples

The following example shows how to define an ISG control policy and attach it to a Layer 2 subscriber authorization group:

```
Router# configure terminal
Router(config)# policy-map type control SampleControlPolicyMap1
R1(config-control-policymap)# class type control always event session-start
R1(config-control-policymap)# exit
Router(config)# l2 subscriber authorization group group1
Router(config-l2-sub-gr)# service-policy type control policy SampleControlPolicyMap1
```

**Related Commands**

Command	Description
<b>l2 subscriber</b>	Creates a Layer 2 subscriber authorization group and enters Layer 2 subscriber group mode.
<b>peer</b>	Defines the target LDP peer PE information.
<b>pseudowire (Layer 2)</b>	Defines the maximum and watermark limits for pseudowires from a peer PE device.



# show bridge-domain

To display bridge-domain information, use the **show bridge-domain** command in privileged EXEC mode.

```
show bridge-domain [[ bridge-id ] [c-mac] [mac {security [address|last violation|statistics]] static address|
table [mac-address|aging-time|count|}] split-horizon [group {group-number|all|none|}] stats]
```

## Syntax Description

<i>bridge-id</i>	(Optional) Identifier for the bridge-domain instance. Integer in the range 1 to Platform_Upper_Bound, where Platform_Upper_Bound is a platform-specific upper limit.
<b>c-mac</b>	(Optional) Displays a specified customer bridge domain.
<b>mac</b>	(Optional) Displays MAC address data. <b>Note</b> The <b>mac</b> keyword is not supported on the Cisco ASR 1000 Series Aggregation Services Router.
<b>security</b>	(Optional) Displays MAC security information.
<b>address</b>	(Optional) Displays addresses. <ul style="list-style-type: none"> <li>When used with the <b>security</b> keyword, displays secure addresses on a specified service instance.</li> <li>When used with the <b>static</b> keyword, displays static addresses in a specified bridge domain.</li> </ul> <b>Note</b> The <b>address</b> keyword is not supported on the Cisco ASR 1000 Series Aggregation Services Router.
<b>last</b>	(Optional) Displays the last violation recorded on the specified bridge domain.
<b>violation</b>	(Optional) Displays information about the last violation recorded on the specified bridge domain.
<b>statistics</b>	(Optional) Displays the number of secured MAC addresses and related statistics.
<b>static</b>	(Optional) Displays static MAC information.
<b>table</b>	(Optional) Displays commands related to the MAC address table.
<i>mac-address</i>	(Optional) Displays the MAC address.

<b>aging-time</b>	(Optional) Displays the time, in minutes, that an entry remains before aging out of the MAC address table.
<b>count</b>	(Optional) Displays the total number of addresses in a bridge-domain table.
<b>split-horizon</b>	(Optional) Displays bridge-domain information for a split-horizon.
<b>group</b>	(Optional) Displays bridge-domain information for a split-horizon group.
<i>group-number</i>	(Optional) Number of a specific split-horizon group for bridge-domain information display.
<b>all</b>	(Optional) Selects all ports in split-horizon groups for bridge-domain information display.
<b>none</b>	(Optional) Selects ports that do not belong to any split-horizon group for bridge-domain information display.
<b>stats</b>	(Optional) Displays bridge-domain statistics.

**Command Modes**

Privileged EXEC (#)

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(33)SRD	This command was introduced.
12.2(33)SRE	This command was modified. The <b>address</b> , <b>aging-time</b> , <b>count</b> , <b>static</b> , and <b>table</b> keywords and the <i>mac-address</i> argument were added.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S to provide support for the Cisco ASR 903 Series Aggregation Services Router. This command was modified to provide support for Ethernet Flow Points (EFPs) on trunk ports (interfaces).
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S. The command was modified to display the MAC address limit for the bridge domain.

**Usage Guidelines**

This command is useful for system monitoring and troubleshooting.

This command is available on both linecards and route processors. To invoke this command on a linecard, log in to the linecard. To invoke this command on a route processor, use the **remote command module** command; for example, **remote command module16 bridge-domain 25**.



**Note** The **remote command** command is not supported on the Cisco ASR 1000 Series Aggregation Services Router.

## Examples

The following is sample output of the **show bridge-domain** command. The output varies slightly by platform. The fields are self-explanatory.

```
Device# show bridge-domain 10

Bridge-domain 10 (2 ports in all)
State: UP                               Mac learning: Enabled
Aging-Timer: 300 second(s)
  GigabitEthernet0/2/2 service instance 10
  GigabitEthernet0/2/3 service instance 10
  MAC address      Policy Tag          Age Pseudoport[VC-lbl,egr-intf]
  0000.5200.010E fwd   dynamic      300 GigabitEthernet0/2/3.EFP10
  0000.5200.010C fwd   dynamic      300 GigabitEthernet0/2/3.EFP10
  0000.5200.0107 fwd   dynamic      299 GigabitEthernet0/2/3.EFP10
  0000.5200.0104 fwd   dynamic      300 GigabitEthernet0/2/3.EFP10
```

The following is sample output where the MAC address limit is displayed:

```
Device# show bridge-domain 100 mac address

Bridge-domain 100 (2 ports in all)
State: UP                               Mac learning: Enabled
Aging-Timer: 5 minute(s)
Maximum address limit: 10240             Current addresses: 300
  Ethernet0/0 service instance 100
  Maximum address limit: 200             Current addresses: 100
1 ports belonging to split-horizon group 1
  Ethernet0/0 service instance 101 (split-horizon group 1)
  Maximum address limit: 300             Current addresses: 150
Software Bridging Info for Bridge Domain 100, contains 2 ports
MAC address      Pseudoport
```

The table below describes the significant fields shown in the display.

**Table 2: show bridge-domain Field Descriptions**

Field	Description
Maximum address limit	The maximum MAC addresses configured for the bridge domain.
Current addresses	The current number of MAC addresses learned for the bridge domain.  <b>Note</b> This information may not display for all platforms.

The following example shows the sample output where information of the Ethernet over Generic Routing Encapsulation (GRE) for a specific bridge domain are displayed:

```
Device# show bridge-domain 10

Bridge-domain 10 (2 ports in all)
State: UP                               Mac learning: Enabled
Aging-Timer: 180 second(s)
    GigabitEthernet2/0/0 service instance 1
    Virtual-Ethernet1 service instance 1
MAC address      Policy    Tag    Age Pseudoport
0000.0000.0002 forward dynamic 177 Virtual-Ethernet1.EFP1 sGRE src:11.1.1.1 dst:1.1.1.2

    0000.0000.0001 forward dynamic 180 GigabitEthernet2/0/0.EFP1
```

#### Related Commands

Command	Description
<b>clear bridge-domain</b>	Clears bridge-domain attributes that are not needed.
<b>remote command</b>	Executes a Cisco 7600 Series Router command directly on the console or a specified module without having to log into the Cisco 7600 Series Router first.
<b>show ethernet service instance</b>	Displays information about Ethernet service instances.
<b>show ethernet service interface</b>	Displays interface-only information about Ethernet customer service instances.

# show cfmpal

To display Ethernet connectivity fault management (CFM) platform adaptation layer (PAL) information, use the **show cfmpal** command in user EXEC or privileged EXEC mode.

**show cfmpal** {*epl*|*info*|*interface type number* {*fwd\_vlan vlan-number*|*level*|*vlan\_list*}}

## Syntax Description

<b>epl</b>	Displays CFM Ethernet private line details.
<b>info</b>	Displays CFM PAL information.
<b>interface</b>	The interface to check the CFM.
<i>type number</i>	The type and the number of the interface. The supported interfaces are FastEthernet, GigabitEthernet, and port channel.
<i>fwd_vlan</i>	Displays the CFM forward VLAN list.
<i>vlan-number</i>	The VLAN number to test the CFM.
<i>level</i>	Displays the CFM level for the interface.
<i>vlan_list</i>	Displays the CFM VLAN list.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

Release	Modification
12.4(22)T	This command was introduced.

## Usage Guidelines

Use the available keywords and arguments to restrict the display to information about a specific Ethernet CFM PAL.

## Examples

The following are sample outputs from the **show cfmpal** command. The fields are self-explanatory.

```
Router# show cfmpal info
CFM enable status Disabled
reg_used_ether_cfmpal_process_rx is Not Used
reg_used_raw_enqueue for LINK_ETHER_CFM is Not Used
flowpoint (fp) count 0
max configured level (MCL) -2
cfmpal cfmpal1 mac addr 0005.0050.9c00,
```

```
CFM multicast mac address BASE 0100.0ccc.ccc0
CFM multicast mac address MASK 0000.0000.000f
Router# show cfm pal epl
flowpoint count 0, MCL -2
Router# show cfm pal interface fastethernet 0/0 level
FastEthernet0/0 is not on epl, it is in transparent level
```

## show ethernet cfm domain

To display information for an Ethernet Connectivity Fault Management (CFM) domain, use the **show ethernet cfm domain** command in privileged EXEC mode.

**show ethernet cfm domain** [*domain-name*] **brief**

### Syntax Description

<i>domain-name</i>	(Optional) String of a maximum length of 154 characters.
<b>brief</b>	(Optional) Displays brief details about the configured maintenance domains.

### Command Default

All information about all the configured domains is displayed when no keyword or argument is used.

### Command Modes

Privileged EXEC (#)

### 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.
12.4(20)T	This command was integrated in a release earlier than Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S. The Source field was added to the command output.
Cisco IOS XE Release 3.5S	This command was modified. The Source field was added to the command output.
Cisco IOS XE Release 3.6S	This command was modified. Information about the local maintenance endpoint (MEP) was added to the Static MEPs counters.

### Usage Guidelines

When a domain name is not specified, information for all domains is displayed.

If a domain name is more than 43 characters in length, 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.

When the **brief** keyword is used, the command output shows the following summary data:

- Domain name
- Domain index
- Domain level
- Number of maintenance associations in the domain
- Archive hold time for the error and continuity check databases for the domain

## Examples

The following is sample output from the **show ethernet cfm domain brief** command.

```
Device# show ethernet cfm domain brief
```

```
Domain Name: XCTEST
Level: 5
Total Services: 1
Services:
  Type Id  Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  XCON N/A Up  Y  10s      Disabled   Disabled   100      Dynamic XCSVC
```

The table below describes the significant fields shown in the display.

**Table 3: show ethernet cfm domain brief Field Descriptions**

Field	Description
Domain Name	Name of the domain.
Level	Maintenance domain level.
Services	Number of services running.

The following is sample output from the **show ethernet cfm domain** command for domain called dom22:

```
Device# show ethernet cfm domain
```

```
Domain Name: dom22
Level: 3
Total Services: 1
Services:
  Type Id  Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  BD-V 10  Dwn Y  100ms n/a          Disabled   100      Static  lvl3
Static MEPs:
  For local MEP on FE1/0/0 service instance 1:
    MPID  Type Id  Static-rmep-Up Crosscheck-Up
    2     BD-V 10  No             n/a
```

The table below describes the significant fields shown in the display.

**Table 4: show ethernet cfm domain Field Descriptions**

Field	Description
Domain Name	Name of the domain.



Field	Description
Level	Maintenance domain level.
Total Services	Number of services running.
Services	The services currently running.
Type Id	Service type and ID.
Dir	Either up (toward the switch) or Dwn (toward the LAN or wire).
CC	Continuity check message (CCM) status (Y for enabled or N for disabled).
CC-int	Time, in milliseconds, between CCMs.
Static-rmep-Up	Status of the remote MEP.
MaxMEP	Number of maximum MEPs allowed.
Source	Static origin or dynamically created.
MA-Name	Name of the maintenance association.
Crosscheck-Up	Status of the cross-check function.

#### Related Commands

Command	Description
<b>show ethernet cfm maintenance-points remote</b>	Displays information about remote maintenance points in the continuity check database.
<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.

## show ethernet cfm errors

To display Connectivity Fault Management (CFM) continuity check error conditions logged on a device since it was last reset or since the log was last cleared, use the **show ethernet cfm errors** command in privileged EXEC mode.

### Cisco Prestandard CFM Draft 1 (CFM D1)

**show ethernet cfm errors** [**domain** *domain-name* | **level** *level-id*]

### CFM IEEE 802.1ag Standard (CFM IEEE) and Cisco ASR 901 Series Aggregation Services Router

**show ethernet cfm errors** [**configuration** | **domain-id** {*mac-address* *domain-name* | *domain-name* | **dns** *dns-name* | **null**} [**service** {**icc** *icc-code* *meg-code* | *maintenance-association-name* | **number** *maintenance-association-number* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} ]]

### Cisco Catalyst 6000 Switches

**show ethernet cfm errors** [**configuration** | **domain-id** {*mac address* | *domain-name* | **dns** *dns-name* | **null**}]

#### Syntax Description

<b>domain</b>	(Optional) Indicates that a maintenance domain is specified.
<i>domain-name</i>	(Optional) String of a maximum of 154 characters in length.
<b>level</b>	(Optional) Indicates that a maintenance level is specified.
<i>level-id</i>	(Optional) Integer from 0 to 7 that identifies the maintenance level.
<b>configuration</b>	(Optional) Displays the configuration error list information; for example, port, VLAN, and error condition.
<b>domain-id</b>	(Optional) Displays error conditions by domain ID.
<i>domain-name</i>	Number of the Domain. The range is from 0 to 65535.
<i>mac-address</i>	(Optional) MAC address of the maintenance domain.
<b>dns</b>	(Optional) Displays a domain name service (DNS).
<i>dns-name</i>	(Optional) String of a maximum of 43 characters in length.
<b>null</b>	Indicates there is not a domain name.

<b>service</b>	(Optional) Displays a maintenance association within the domain.
<b>icc</b>	(Optional) Displays error conditions by the ITU-T Y.1731 Carrier Code (ICC)-based maintenance entity group (MEG) identifier.
<i>icc-code</i>	(Optional) String that identifies the ICC. String of a maximum length of six characters.
<i>meg-code</i>	(Optional) String that identifies the unique MEG code. String of a maximum length of 12 characters.
<i>maintenance-association-name</i>	(Optional) String that identifies the maintenance association.
<i>number</i>	(Optional) Specifies a maintenance association by a numerical ID.
<i>maintenance-association-number</i>	(Optional) Integer that identifies the maintenance association.
<b>vlan-id</b>	(Optional) Displays a VLAN.
<i>vlan-id</i>	(Optional) Integer from 1 to 4094 that identifies the VLAN.
<b>vpn-id</b>	(Optional) Displays a VPN.
<i>vpn-id</i>	(Optional) Integer from 1 to 32767 that identifies the VPN.

**Command Default**

In CFM IEEE, errors for all domains are displayed when no maintenance domain is specified.

In CFM D1, errors for all domains and all levels are displayed when no maintenance domain or maintenance level is specified.

**Command Modes**

Privileged EXEC (#)

**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.

Release	Modification
12.2(33)SX12	This command was integrated into Cisco IOS Release 12.2(33)SX12.
15.0(1)XA	This command was integrated into Cisco IOS Release 15.0(1)XA.
12.2(54)SE	This command was integrated into Cisco IOS Release 12.2(54)SE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The order of the columns shown in the display was rearranged, and the <b>icc</b> keyword was added to provide support for the ICC-based MEG identifier.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
Cisco IOS XE Release 3.6S	This command was modified to include information about the local maintenance endpoint (MEP).
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

### Usage Guidelines

Errors that are logged and displayed by the **show ethernet cfm errors** command vary according to the version of CFM in use. Errors include the following:

- MEP-Down—Maintenance endpoint (MEP) timed out or is advertising a 0 lifetime.
- Configuration Error—A continuity check message (CCM) is received that has a maintenance point ID (MPID) matching the local device, but the source MAC address is different.
- Forwarding Loop—A CCM is received that has the same MPID and same MAC address as the local device.
- Cross-connected—A CCM is received and the service ID does not match the service ID configured on the device for that VLAN.
- Cross-check Missing MEP—The cross-checking delay timer has expired, and the configured remote MEP did not come up.
- Cross-check Unknown MEP—An unexpected remote MEP came up.
- Receive AIS—A MEP detects a mismerge, which is an unexpected MEP condition, or a signal fail condition resulting in peer MEPs receiving an alarm indication signal (AIS) frame.

Error conditions are kept in a log for the duration of the archive hold time configured on the maintenance domain or until the error condition is cleared, whichever occurs first.

## Examples

The following is sample output from the **show ethernet cfm errors** command:

Device# **show ethernet cfm errors**

```

-----
MPID Domain Id          Mac Address      Type  Id
      MAName          Reason        Lvl  Age
      Local MEP Identifier
-----
2      abc              0000.0000.0000   BD-V  10
      lvl3              Remote MEP missing 3    2s
      Mpid: 1, Domain: abc, MA: lvl3

1      abc              aabb.cc00.2901   BD-V  10
      lvl3              Unknown MEP       3    2s      Mpid: 1,
Domain: abc, MA: lvl3

```

The following is sample output from the **show ethernet cfm errors** command when MEPs are configured for two Maintenance Associations (MAs), MA1 and MA2, and MA2 is configured as an alias to MA1 using the **alias** command:

Device# **show ethernet cfm errors**

```

-----
MPID Domain Id          Mac Address      Type  Id
      MA Name          Reason        Lvl  Age
      Local MEP Info
-----
21      lvl3              aabb.cc00.2a03   BD-V  10
      ma1              Receive RDI       3    0s
      MPID: 11 Domain: lvl3 MA: ma1

10      lvl3              0000.0000.0000   BD-V  20
      ma2 (ma1)         RMEP missing      3    0s
      MPID: 21 Domain: lvl3 MA: ma2 (ma1)

2      lvl3              aabb.cc00.2c02   BD-V  10
      ma2              Crossconnect Err  3    0s
      MPID: 11 Domain: lvl3 MA: ma1

2      lvl3              aabb.cc00.2c02   BD-V  20
      ma2              Crossconnect Err  3    0s
      MPID: 21 Domain: lvl3 MA: ma2 (ma1)

```

The table below describes the significant fields shown in the display.

**Table 5: show ethernet cfm errors Field Descriptions**

Field	Description
MPID	Identifier of the MEP on which the error occurred.
Domain Id	Identifier of the domain affected by the error.
Mac Address	MAC address of the remote MEP on which the error occurred.
Type	Type of MEP.
Id	Identifier of the VLAN on which the error occurred.

Field	Description
MAName	Name of the maintenance association where the error occurred.
Reason	Explanation of why the error occurred.
Lvl	Maintenance level at which the error occurred.
Age	Time (in seconds) that the error has been in the error database.
Local MEP Identifier	Identifier of the local maintenance endpoint.

The following is sample output from the **show ethernet cfm errors** command when the optional **configuration** keyword is used:

```
Device# show ethernet cfm errors configuration
```

```
-----
CFM Interface      Type  Id    Level  Error type
-----
Fe0/0/0            VLAN  100   1      CFMLeak
```

The table below describes the significant fields shown in the display.

**Table 6: show ethernet cfm errors configuration Field Descriptions**

Field	Description
CFM Interface	CFM supported interface on which the error occurred.
Type	Type of MEP.
Id	Identifier of the VLAN on which the error occurred.
Level	Maintenance level at which the error occurred.
Error type	Type of error.

The following is sample output from the **show ethernet cfm errors** command for CFM error conditions at maintenance level 3:

```
Device# show ethernet cfm errors level 3
```

```
Level Vlan MPID Remote MAC      Reason          Service ID
5     102  40  aabb.cc00.ca10  Receive AIS     service test
```

The table below describes the significant fields shown in the display.

**Table 7: show ethernet cfm errors Field Descriptions**

Field	Description
Level	Maintenance level at which the error occurred.
Vlan	VLAN on which the error occurred.
MPID	Identifier of the MEP on which the error occurred.
Remote MAC	The MAC address of the remote MEP on which the error occurred.
Reason	Explanation of why the error occurred.
Service ID	Identifier of the entity affected by the error.

**Related Commands**

Command	Description
<b>alias</b>	Configures an MA alias within a domain.
<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.







## show ethernet cfm maintenance-points local through weight

---

- [show ethernet cfm maintenance-points local, page 370](#)
- [show ethernet cfm maintenance-points remote, page 376](#)
- [show ethernet cfm maintenance-points remote crosscheck, page 381](#)
- [show ethernet cfm maintenance-points remote detail, page 385](#)
- [show ethernet cfm mpdb, page 389](#)
- [show ethernet cfm pm, page 393](#)
- [show ethernet cfm smep, page 395](#)
- [show ethernet cfm statistics, page 397](#)
- [show ethernet cfm traceroute-cache, page 400](#)
- [show ethernet event microwave statistics, page 403](#)
- [show ethernet event microwave status, page 404](#)
- [show ethernet lmi, page 406](#)
- [show ethernet loopback, page 413](#)
- [show ethernet mac-tunnel engine slot, page 415](#)
- [show ethernet oam debug link-monitor, page 416](#)
- [show ethernet oam discovery, page 418](#)
- [show ethernet oam runtime, page 421](#)
- [show ethernet oam statistics, page 424](#)
- [show ethernet oam status, page 427](#)
- [show ethernet oam summary, page 431](#)
- [show ethernet ring g8032 brief, page 433](#)
- [show ethernet ring g8032 configuration, page 435](#)
- [show ethernet ring g8032 port status, page 437](#)

- [show ethernet ring g8032 profile, page 438](#)
- [show ethernet ring g8032 statistics, page 439](#)
- [show ethernet ring g8032 status, page 441](#)
- [show ethernet ring g8032 summary, page 444](#)
- [show ethernet ring g8032 trace, page 446](#)
- [show ethernet service dynamic, page 447](#)
- [show ethernet service evc, page 450](#)
- [show ethernet service instance, page 452](#)
- [show ethernet service interface, page 458](#)
- [show ethernet service mac-tunnel, page 461](#)
- [show lacp, page 464](#)
- [show lldp, page 471](#)
- [show nmsp, page 478](#)
- [show ptp clock dataset, page 482](#)
- [show ptp clock dataset parent, page 485](#)
- [show ptp clock dataset time-properties, page 487](#)
- [show ptp clock running, page 489](#)
- [show ptp port dataset foreign-master, page 491](#)
- [show ptp port dataset port, page 493](#)
- [shutdown \(bridge-domain\), page 495](#)
- [snmp-server enable traps ethernet cfm alarm, page 496](#)
- [snmp-server enable traps ethernet cfm cc, page 497](#)
- [snmp-server enable traps ethernet cfm crosscheck, page 501](#)
- [snmp-server enable traps ethernet evc, page 504](#)
- [snmp-server enable traps ether-oam, page 505](#)
- [snmp-server host traps evc, page 506](#)
- [source template \(eoam\), page 507](#)
- [status decoupled, page 509](#)
- [status peer topology dual-homed, page 511](#)
- [sync interval, page 513](#)
- [template \(eoam\), page 515](#)
- [timer \(Ethernet ring\), page 517](#)
- [tod, page 518](#)

- [traceroute ethernet, page 520](#)
- [traceroute ethernet evc, page 524](#)
- [traceroute ethernet vlan, page 526](#)
- [transport ipv4 \(PTP\), page 528](#)
- [uni count, page 530](#)
- [weight \(srvs instance\), page 532](#)

# show ethernet cfm maintenance-points local

To display information about local Connectivity Fault Management (CFM) maintenance points that are configured on a device, use the **show ethernet cfm maintenance-points local** command in privileged EXEC mode.

**show ethernet cfm maintenance-points local** [**detail**] [**mep** | **mip**] [**domain** *domain-name* | **interface** *type number* | **level** *level-id* | **evc** *evc-name*] {**static** | **dynamic**}

## Syntax Description

<b>detail</b>	(Optional) Displays detailed output.
<b>mep</b>	(Optional) Indicates that a maintenance endpoint (MEP) is specified.
<b>mip</b>	(Optional) Indicates that a maintenance intermediate point (MIP) is specified.
<b>domain</b>	(Optional) Indicates that a maintenance domain is specified.
<i>domain-name</i>	(Optional) String of a maximum length of 154 characters.
<b>interface</b>	(Optional) Indicates that an interface is specified.
<i>type number</i>	(Optional) Type and number of the interface.
<b>level</b>	(Optional) Indicates that a maintenance level is specified.
<i>level-id</i>	(Optional) Integer from 0 to 7 that identifies the maintenance level.
<b>evc</b>	(Optional) Indicates that an Ethernet virtual circuit (EVC) is specified. <ul style="list-style-type: none"> <li>The <b>evc</b> keyword is not supported in Cisco IOS Release 12.2(54)SE and Cisco IOS Release 12.2(50)SY.</li> </ul>
<i>evc-name</i>	(Optional) Identifier for an EVC. <ul style="list-style-type: none"> <li>The <i>evc-name</i> argument is not supported in Cisco IOS Release 12.2(54)SE and Cisco IOS Release 12.2(50)SY.</li> </ul>
<b>static</b>	(Optional) Indicates configuration through the CLI.

<b>dynamic</b>	(Optional) Indicates configuration through a dynamic session or an accounting, authentication, and authorization (AAA) server.
----------------	--

**Command Default** When none of the optional keywords and arguments is specified, information about all the maintenance points on the device is shown.

**Command Modes** Privileged EXEC (#)

<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)SRD	The <b>detail</b> and <b>evc</b> keywords and the <i>evc-name</i> argument were added.
	12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.  • Support was removed for the <b>evc</b> keyword and <i>evc-name</i> argument in this release.
	15.0(1)XA	This command was modified. Support was removed for the <b>evc</b> keyword and <i>evc-name</i> argument in this release.
	12.2(54)SE	This command was integrated into Cisco IOS Release 12.2(54)SE.
	15.1(2)S	This command was modified. The <b>static</b> and <b>dynamic</b> keywords were added and the command was integrated into Cisco IOS Release 15.1(2)S.
	12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY. Support was removed for the <b>evc</b> keyword, the <i>evc-name</i> argument, the <b>static</b> keyword and the <b>dynamic</b> keyword.
	15.2(1)S	This command was modified. A heading called "Ofld" was added to the output, and the ITU Carrier Code (ICC)-based name was displayed, if applicable. Also, the output was modified to a single-column format when the optional <b>detail</b> keyword was used.
	Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
	15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
	15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

**Usage Guidelines**

The **show ethernet cfm maintenance-points local** command allows you to filter the command output. You can display information about maintenance points, as follows:

- Independent of domain or interface
- On a particular interface independent of domain
- On a particular interface belonging to a given domain
- Belonging to a given domain independent of interface

The display may also be restricted to either MEPs or MIPs.

If a domain name is more than 43 characters in length, 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.

**Examples**

The following is sample output from the **show ethernet cfm maintenance-points local** command:

```
Device# show ethernet cfm maintenance-points local
```

```
Local MEPs:
```

MPID	Domain Name	Lvl	MacAddress	Type	CC
Ofld	Domain Id	Dir	Port	Id	
	MA Name		SrvInst	Source	
	EVC name				
41	L4	4	aabb.cc01.9100	BD-V	Y
No	null	Down	Et0/0	10	
	icc icc1234567890	N/A		Static	
	evc1				

```
Total Local MEPs: 1
```

```
Local MIPs: None
```

The following is sample output from the **show ethernet cfm maintenance-points local** command when local MEPs are configured for two MAs, MA1 and MA2, and MA2 is configured as an alias for MA1 using the **alias** command:

```
Device# show ethernet cfm maintenance-points local
```

```
Local MEPs:
```

MPID	Domain Name	Lvl	MacAddress	Type	CC
Ofld	Domain Id	Dir	Port	Id	
	MA Name		SrvInst	Source	
	EVC name				
11	lv13	3	aabb.cc00.2a02	BD-V	Y
No	lv13	Up	Et2/0	10	
	ma1		1	Static	
	evc10				
21	lv13	3	aabb.cc00.2a03	BD-V	Y
No	lv13	Up	Et3/0	20	
	ma2 (ma1)		N/A	Static	
	evc20				

```
Total Local MEPs: 2
```

Local MIPs: None

The following is sample output from the **show ethernet cfm maintenance-points local detail** command. Depending on which features are enabled in your network, the output may vary slightly from what is shown.

Device# **show ethernet cfm maintenance-points local detail**

```
Local MEPs:
-----
MPID: 300
DomainName: OUT
MA Name: out300
Level: 7
Direction: Down
EVC: evc300
Bridge Domain: 300
Service Instance: 300
Interface: Et1/0
CC Offload: No
CC Offload sampling: 10
CC-Status: Enabled
CC Loss Threshold: 3
MAC: aabb.cc00.0301
LCK-Status: Enabled
LCK Period: 60000(ms)
LCK Expiry Threshold: 3.5
Level to transmit LCK: Default
Defect Condition: No Defect
presentRDI: FALSE
AIS-Status: Enabled
AIS Period: 60000(ms)
AIS Expiry Threshold: 3.5
Level to transmit AIS: Default
Suppress Alarm configuration: Enabled
Suppressing Alarms: No
Source: Static
```

The following is sample output from the **show ethernet cfm maintenance-points local dynamic** command. Note the “Source” field where the type of configuration is indicated.

Device# **show ethernet cfm maintenance-points local dynamic**

```
Local MEPs:
-----
MPID Domain Name                               Lvl  MacAddress  Type CC
Ofld Domain Id                               Dir   Port       Id
      MA Name                               SrvcInst    Source
      EVC name
-----
77  XCTEST                                     5    aabb.cc00.d399 XCON Y
No  XCTEST                                     Up    Et0/0         N/A
    XCSVC                                     3                      Dynamic
    XCEVC
```

Total Local MEPs: 1

```
Local MIPs:
* = MIP Manually Configured
```

Level	Port	MacAddress	SrvcInst	Type	Id	Source
7	Et0/0	aabb.cc00.d399	3	XCON	N/A	Dynamic

Total Local MIPs: 1

The table below describes the significant fields shown in the display.

**Table 8: show ethernet cfm maintenance-points local Field Descriptions**

Field	Description
MPID Domain Name	Identifier of the maintenance point domain name.
Lvl	Maintenance level where the maintenance point is configured.
MacAddress	MAC address of the maintenance point.
Type	Type of MEP.
CC	Continuity check operational status.
Ofld	Indicates whether the MEP is offloaded to the hardware.
Domain Id	Identifier of the offload domain.
Dir	Direction in which the maintenance point is facing.
Port	Port MEP.
Id	Identifier of the VLAN.
MA Name	Name of the maintenance association.
SrvInst	MAC address of the MEP.
Source	Static or Dynamic.
EVC name	Name of the EVC.
icc	ITU-T Y.1731 ITU Carrier Code (ICC) identifier. Also displays the unique maintenance entity group (MEG) code (UMC).

**Related Commands**

Command	Description
<b>alias</b>	Configures a CFM MA as an alias for another MA in the same domain.
<b>show ethernet cfm maintenance-points remote</b>	Displays information about RMEPs configured statically in the MEP list and their status in the CCDB.
<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 CCDB.





## show ethernet cfm maintenance-points remote

To display information about remote Connectivity Fault Management (CFM) maintenance endpoints (RMEPs) that are configured statically in the MEP list and their status in the continuity check database (CCDB), use the **show ethernet cfm maintenance-points remote** command in privileged EXEC mode.

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

**show ethernet cfm maintenance-points remote** [**domain** *domain-name* | **level** *level-id*]

### CFM IEEE 802.1ag Standard (CFM IEEE)

**show ethernet cfm maintenance-points remote** [**domain** *domain-name* | [[**crosscheck** | **static**] [**domain** *domain-name* | **mpid** *mpid* [**domain** *domain-name*]] [**port** | **vlan** *vlan-id*]]]

### Cisco ASR 901 Series Aggregation Services Router and Cisco ASR 1000 Series Aggregation Services Router

**show ethernet cfm maintenance-points remote static mpid** *mpid* **domain** [**service** {*short-ma-name* | **icc** *icc-code* *meg-id* | **number** *ma-number* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*}]

#### Syntax Description

<b>domain</b> <i>domain-name</i>	(Optional) Displays a specific maintenance domain. String of a maximum of 154 characters in length.
<b>level</b> <i>level-id</i>	(Optional) Displays a specific maintenance level. Specifies an integer from 0 to 7 that identifies the maintenance level.
<b>crosscheck</b>	(Optional) Displays the Mep-Up status from the D1 cross-check function.
<b>static</b>	(Optional) Displays the Mep-Up status from the continuity-check static RMEP function.
<b>mpid</b> <i>mpid</i>	Displays a remote maintenance point. Specifies an integer from 0 to 8191 that identifies the maintenance point.
<b>service</b>	(Optional) Specifies the maintenance association (MA) within the domain.
<i>short-ma-name</i>	The short-name identifier for the MA service.
<b>icc</b> <i>icc-code</i> <i>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>	Specifies the MA number. Range: 0 to 65535.

<b>vlan-id</b> <i>vlan-id</i>	Specifies the primary VLAN ID. Range: 1 to 4094.
<b>vpn-id</b> <i>vpn-id</i>	Specifies the VPN ID. Range: 1 to 32767.

**Command Default** When no domain or a maintenance level (CFM D1 only) is specified, all CCDB MEP entries are displayed.

**Command Modes** Privileged EXEC (#)

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)SRB	This command was modified. The output was enhanced to include the port state values of REMOTE_EE, LOCAL_EE, and TEST.
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.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
Cisco IOS XE Release 3.6S	This command was modified to include information about the local maintenance endpoint (MEP) when the <b>static</b> keyword is used.
Cisco IOS XE Release 3.7S	This command was modified.  The <b>port</b> , <b>vlan</b> , and <b>evc</b> keywords were deprecated. You must specify the MA service via the <i>ma-fmt short-ma-name</i> identifier.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

**Usage Guidelines** 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.

When no maintenance domain is specified, all entries are displayed; otherwise, only entries belonging to the specified domain or level (CFM D1 only) are shown.

**Examples**

The following is sample output from the **show ethernet cfm maintenance-points remote** command:

```
Device# show ethernet cfm maintenance-points remote
```

```
-----
MPID  Domain Name                      MacAddress      IfSt  PtSt
Lvl   Domain ID                        Ingress
RDI   MA Name                          Type Id         SrvcInst
-----
42    L4                               aabb.cc01.9310  Up    Up
4     null                             Et0/0.10
-     icc icc1234567890                 BD-V 10         N/A
Total Remote MEPs: 1
```

The following is the sample output from the **show ethernet cfm maintenance-points remote** command when remote MEPs are configured for two MAs, MA1 and MA2, and MA2 is configured as an alias for MA1 using the **alias** command:

```
Device# show ethernet cfm maintenance-points remote domain lvl3 service ma1
```

```
-----
MPID  Domain Name                      MacAddress      IfSt  PtSt
Lvl   Domain ID                        Ingress
RDI   MA Name                          Type Id         SrvcInst
      EVC Name                        Age
      Local MEP Info
-----
21    lvl3                               aabb.cc00.2a03  Up    Up
3     lvl3                               Et0/0
-     ma1                               BD-V 10         1
      evc10                             0s
      MPID: 11 Domain: lvl3 MA: ma1
1     lvl3                               aabb.cc00.2b02  Up    Up
3     lvl3                               Et0/0
-     ma1                               BD-V 10         1
      evc10                             0s
      MPID: 11 Domain: lvl3 MA: ma1
11    lvl3                               aabb.cc00.2a02  Up    Up
3     lvl3                               Et1/0
-     ma2 (ma1)                         BD-V 20         1
      evc20                             0s
      MPID: 21 Domain: lvl3 MA: ma2 (ma1)
1     lvl3                               aabb.cc00.2b02  Up    Up
3     lvl3                               Et1/0
-     ma2 (ma1)                         BD-V 20         1
      evc20                             0s
      MPID: 21 Domain: lvl3 MA: ma2 (ma1)
```

```
Total Remote MEPs: 4
```

The table below describes the significant fields shown in the display.

**Table 9: show ethernet cfm maintenance-points remote Field Descriptions**

Field	Description
MPID	Identifier of the MEP.
Lvl	Maintenance level.
RDI	Remote defect indication (RDI) messages on the maintenance point.

Field	Description
Domain Name	Name of the domain.
Domain ID	MAC address of the MEP.
MA Name	Name of the MA.
Mac Address	MAC address of the MEP.
Ingress	Port on which the packet is received.
Type Id	Type of service.
IfSt	Operational state of the interface.
PtSt	Operational state of the port MEP. Values are: <ul style="list-style-type: none"> <li>• Up—Operational.</li> <li>• DOWN—Not operational.</li> <li>• ADMINDOWN—Administratively down.</li> <li>• REMOTE_EE—Encountered excessive number of remote errors.</li> <li>• LOCAL_EE—Encountered excessive number of local errors.</li> <li>• TEST—Test state.</li> </ul>
SrvInst	MAC address of the MEP.
Age	Amount of time, in seconds, the entry has been in the database.

The following is sample output from the **show ethernet cfm maintenance-points remote static** command:

Device# **show ethernet cfm maintenance-points remote static**

```

-----
MPID Domain Name                               Lvl Type Id      Mep-Up
      MA Name
      Local MEP Info
-----
  2 abc                                           7 BD-V 10        No
    lvl3

```

The table below describes the significant fields shown in the display.

**Table 10: show ethernet cfm maintenance-points remote static Field Descriptions**

Field	Description
MPID	Identifier of the maintenance point.
Domain Name	Name of the domain.
Lvl	Maintenance level where the maintenance point is configured.
Type Id	Type of service.
Mep-Up	Operational status of the MEP.
MA Name	Name of the MA.
Local MEP Identifier	Identifier of the local maintenance endpoint.

**Related Commands**

Command	Description
<b>alias</b>	Configures an MA alias within a domain.
<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.

# show ethernet cfm maintenance-points remote crosscheck

To display information about remote Connectivity Fault Management (CFM) maintenance points configured that are statically in a cross-check list, use the **show ethernet cfm maintenance-points remote crosscheck** command in privileged EXEC mode.

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

**show ethernet cfm maintenance-points remote crosscheck** [**mpid** *id* | **mac** *mac-address*] [**domain** *domain-name* | **level** *level-id* ] [**evc** *evc-name* | **vlan** *vlan-id*]

## CFM IEEE 802.1ag Standard (CFM IEEE)

**show ethernet cfm maintenance-points remote crosscheck**[**domain** *domain-name* | **mpid** *id* [**domain** *domain-name* ]][**evc** *evc-name* | **port** | **vlan** *vlan-id*]

## Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

**show ethernet cfm maintenance-points remote crosscheck mpid** *mpid* {**domain** *domain-name* {**service** {*ma-name* | **number** *ma-number* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id* | **evc** *evc-name* | **port** | **vlan** *vlan-id*} **evc** *evc-name* | **port** | **vlan** | *vlan-id*}}

## Cisco ASR 901 Series Aggregation Services Router and Cisco ASR 1000 Series Aggregation Services Router

**show ethernet cfm maintenance-points remote crosscheck** [**mpid** *mpid*] **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>mpid</b> <i>mpid</i>	Specifies a MEP identifier (MPID) and value. Range: 1 to 8191.
<b>mac</b> <i>mac-address</i>	(Optional) Specifies the MAC address of the remote maintenance point, in the format abcd.abcd.abcd.
<b>domain</b> <i>domain-name</i>	(Optional) Specifies the domain where the destination MEP resides. Maximum: 154 characters.
<b>level</b> <i>level-id</i>	(Optional) Indicates that a maintenance level is specified. Integer from 0 to 7.
<b>evc</b> <i>evc-name</i>	(Optional) String that associates an Ethernet virtual connection (EVC) to the service instance. Maximum: 100 bytes.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies a VLAN for cross-checking. Integer from 1 to 4094 that identifies the VLAN.

<b>port</b>	(Optional) Specifies a DOWN service direction with no VLAN associations (untagged).
<b>service</b>	(Optional) Specifies the maintenance association (MA) within the domain.
<i>short-ma-name</i>	(Optional) 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>	(Optional) 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>	(Optional) The MA number. Range: 0 to 65535.
<b>vlan-id</b> <i>vlan-id</i>	(Optional) The primary VLAN ID. Range: 1 to 4094.
<b>vpn-id</b> <i>vpn-id</i>	(Optional) The VPN ID. Range: 1 to 32767.

**Command Default**

When no options are specified, maintenance point IDs (MPIDs), MAC addresses, domains, levels, and VLANs for all maintenance points on the list are displayed.

**Command Modes**

Privileged EXEC (#)

**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)SRD	The <b>evc</b> <i>evc-name</i> keyword-argument pair was added on the Cisco 7600 series Route Switch Processor 720 (RSP 720) and the Cisco 7600 series Supervisor Engine 720.
12.2(33)SRE	This command was modified. Support for the <b>port</b> keyword was added.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY. The support for the <b>evc</b> <i>evc-name</i> keyword-argument pair was removed.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
Cisco IOS XE Release 3.6S	This command was modified to include information about the local maintenance endpoint (MEP).



Release	Modification
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
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.

## Examples

The following is sample output from the **show ethernet cfm maintenance-points remote crosscheck** command:

```
Device# show ethernet cfm maintenance-points remote crosscheck
```

```
-----
MPID Domain Name                               Lvl Type Id      Mep-Up
   MA Name
   Local MEP Info
-----
  2 abc                                           7 BD-V 10       No
   lvl3
```

The following is sample output from the **show ethernet cfm maintenance-points remote crosscheck** command when remote MEPs are configured for two MAs, MA1 and MA2, and MA2 is configured as an alias for MA1 using the **alias** command:

```
Device# show ethernet cfm maintenance-points remote crosscheck
```

```
-----
MPID Domain Name                               Lvl Type Id      Mep-Up
   MA Name
   Local MEP Info
-----
  1 lvl3                                           3 BD-V 20       n/a
   ma2 (ma1)
   N/A
 11 lvl3                                           3 BD-V 20       n/a
   ma2 (ma1)
   N/A
 10 lvl3                                           3 BD-V 20       n/a
   ma2 (ma1)
   N/A
```

The table below describes the significant fields shown in the display.

**Table 11: show ethernet cfm maintenance-points remote crosscheck Field Descriptions**

Field	Description
MPID	Identifier of the maintenance point.
Domain Name	Name of the domain.

Field	Description
Lvl	Maintenance level where the maintenance point is configured.
Type Id	Type of service.
Mep-Up	Operational status of the MEP.
MA Name	Name of the MA.
Local MEP Identifier	Identifier of the local maintenance endpoint.

The following is sample output from the **show ethernet cfm maintenance-points remote crosscheck** command for maintenance points at maintenance level 4:

```
Device# show ethernet cfm maintenance-points remote crosscheck

-----
MPID Domain Name                               Lvl Type Id      Mep-Up
      MA Name
      Local MEP Info
-----
 12  lvl3
     ma2                               3 BD-V 20        Yes
     N/A
 11  lvl3                               3 BD-V 20        No
     ma2
     N/A
```

## Related Commands

Command	Description
<b>alias</b>	Configures an MA alias within a domain.
<b>show ethernet cfm maintenance-points local</b>	Displays information about maintenance points configured on a device.
<b>show ethernet cfm maintenance-points remote</b>	Displays information about remote maintenance points in the continuity check database.
<b>show ethernet cfm maintenance-points remote detail</b>	Displays information about a remote maintenance point in the continuity check database.

# show ethernet cfm maintenance-points remote detail

To display information about a remote maintenance point in the continuity check database, use the **show ethernet cfm maintenance-points remote detail** command in privileged EXEC mode.

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

```
show ethernet cfm maintenance-points remote detail {mac mac-address} mpid mpid} [domain domain-name|
level level-id] [evc evc-name| srv-instance service-name| vlan vlan-id]
```

## CFM IEEE 802.1ag (CFM IEEE)

```
show ethernet cfm maintenance-points remote detail {mac mac-address} mpid mpid} [domain domain-name|
evc evc-name| port| vlan vlan-id]
```

## Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

```
show ethernet cfm maintenance-points remote detail mpid mpid {domain domain-name {service {ma-name|
number ma-num| vlan-id vlan-id| vpn-id vpn-id}| evc evc-name| port| vlan vlan-id}| evc evc-name| port|
vlan vlan-id}
```

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

```
show ethernet cfm maintenance-points remote detail {mac mac-address} mpid mpid} [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>mac</b> <i>mac-address</i>	Displays a remote MAC address. MAC address of the remote maintenance point, in the format abcd.abcd.abcd.
<b>mpid</b> <i>mpid</i>	Displays a remote maintenance point. Specifies an integer from 0 to 8191 that identifies the maintenance point.
<b>domain</b> <i>domain-name</i>	(Optional) Displays a specific maintenance domain. String of a maximum of 154 characters in length.
<b>level</b> <i>level-id</i>	(Optional) Displays a specific maintenance level. Specifies an integer from 0 to 7 that identifies the maintenance level.
<b>evc</b> <i>evc-name</i>	(Optional) String that associates an Ethernet virtual connection (EVC) to the service instance. Maximum: 100 bytes.

<b>srv-instance</b> <i>service-name</i>	(Optional) Displays a customer service instance. Specifies a string that identifies the service instance.
<b>vlan</b> <i>vlan-id</i>	(Optional) Indicates a VLAN for cross-checking. Integer from 1 to 4094 that identifies the VLAN.
<b>port</b>	(Optional) Specifies a DOWN service direction with no VLAN associations (untagged).
<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**

When no options are specified, all remote MEPs matching the specified MAC address or maintenance point ID (MPID) are displayed.

**Command Modes**

Privileged EXEC (#)

**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)SRD	The command output was modified to display detailed information about receive remote defect indication (RDI) and EVCs. The <b>evc</b> keyword was introduced.
12.2(33)SX12	This command was integrated into Cisco IOS Release 12.2(33)SX12.
15.0(1)XA	This command was modified. Support for the <b>evc</b> keyword was added.

Release	Modification
12.2(54)SE	This command was modified. Support for the <b>number</b> , <b>service</b> , <b>vlan-id</b> , and <b>vpn-id</b> keywords and the <i>ma-name</i> , <i>ma-num</i> , and <i>vpn-id</i> arguments was added.
12.2(50)SY	This command was integrated. The <b>number</b> , <b>service</b> , <b>vlan-id</b> , and <b>vpn-id</b> keywords and the <i>ma-name</i> , <i>ma-num</i> , and <i>vpn-id</i> arguments were not supported in this release.
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

Use this command to obtain information about a specific maintenance point by specifying its MPID or to obtain information about all maintenance points that have a particular MAC address.

When a maintenance domain is not specified, all matching maintenance points, independent of their levels (CFM D1 only), are displayed; otherwise, only maintenance points at the specified maintenance domain are shown.

### Examples

The following is sample output from the **show ethernet cfm maintenance-points remote detail** command using the **mpid** option:

```
Device# show ethernet cfm maintenance-points remote detail mpid 401

Version: IEEE-CFM
MAC Address: aabb.cc03.bb99
Domain Name: Domain_L5
MA Name: cust_500_15
Level: 5
VLAN: 9
MPID: 401
Sender Chassis ID: Device3-cfm
Incoming Port(s): Ethernet0/0.9
CC Lifetime(sec): 35
Age of Last CC Message(sec): 10
CC Packet Statistics: 91/0 (Received/Error)
MEP interface status: Up
MEP port status: Up
Receive RDI: FALSE
Device#
```

The table below describes the significant fields shown in the display.

**Table 12: show ethernet cfm maintenance-points remote detail Field Descriptions**

Field	Description
Version	Version of the CFM that is running.

Field	Description
MAC Address	MAC address of the remote MEP.
Domain Name	Name of the domain.
MA Name	Name of the MA.
Level	Maintenance domain level.
VLAN	Configured VLAN.
MPID	Identifier of the maintenance point.
Sender Chassis ID	Name of the other switch or device when the sender ID is configured on that device.
Incoming Port(s)	Identifier of the port that receives the message.
CC Lifetime(sec)	Amount of time, in seconds, that the message should remain in the database before being purged.
Age of Last CC Message(sec)	Amount of time, in seconds, the previous continuity check message (CCM) has been in the database.
CC Packet Statistics	Number of packets received and number of packets with errors.
MEP interface status	Operational state of the MEP interface.
MEP port status	Operational state of the MEP port.
Receive RDI	Receive status of remote defect indication (RDI) messages on the maintenance point.

#### 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</b>	Displays information about remote maintenance points in the continuity check database.
<b>show ethernet cfm maintenance-points remote crosscheck</b>	Displays information about remote maintenance points configured statically in a cross-check list.

# show ethernet cfm mpdb

To display the contents of a maintenance intermediate point (MIP) continuity check database (CCDB), use the **show ethernet cfm mpdb** command in privileged EXEC mode.

**show ethernet cfm mpdb** [**domain-id** {*mac-address* *domain-number* | **dns** *dns-name* | **null**} [**service** {**icc** *icc-code* *meg-code* | *ma-name* | **number** *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*}]]

## Syntax Description

<b>domain-id</b>	(Optional) Displays by domain ID.
<i>mac-address</i>	MAC address of the maintenance domain.
<i>domain-number</i>	Domain number. The range is from 0 to 65535.
<i>domain-name</i>	String of a maximum of 43 characters that identifies the domain.
<b>dns</b>	Specifies a domain name service (DNS).
<i>dns-name</i>	String of a maximum of 43 characters that identifies the DNS.
<b>null</b>	Indicates there is not a domain name.
<b>service</b>	(Optional) Specifies a maintenance association within the domain.
<b>icc</b>	Displays the CCDB contents on the basis of the ITU-T Y.1731 Carrier Code (ICC)-based maintenance entity group (MEG) identifier.
<i>icc-code</i>	String that identifies the ICC. String of a maximum of six characters.
<i>meg-code</i>	String that identifies the unique MEG code. String of a maximum of 12 characters.
<i>ma-name</i>	String that identifies a maintenance association.
<i>number</i>	Specifies a maintenance association by a numerical ID.
<i>ma-num</i>	Integer from 0 to 65535 that identifies the maintenance association.
<b>vlan-id</b>	Specifies a VLAN.

<i>vlan-id</i>	Integer from 1 to 4094 that identifies the VLAN.
<b>vpn-id</b>	Specifies a virtual private network (VPN).
<i>vpn-id</i>	Integer from 1 to 32767 that identifies the VPN.

**Command Default** When no maintenance domain is specified, all entries are displayed.

**Command Modes** Privileged EXEC (#)

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.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
12.2(54)SE	This command was integrated into Cisco IOS Release 12.2(54)SE.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The <b>icc</b> keyword was added to provide support for the ICC-based MEG identifier.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** Use this command to display cataloged information received from MEPs.

**Examples** The following example is sample output from the **show ethernet cfm mpdb** command.

Device# **show ethernet cfm mpdb**

\* = Can Ping/Traceroute to MEP

MPID	Domain Name	MacAddress	Version
Lvl	Domain ID	Ingress	
Expd	MA Name	Type Id	SrvInst
	EVC Name		Age
220 *	Domain_L5	aabb.cc03.b999	IEEE-CFM
5	Domain_L5	Et0/0.1	
EXPD	cust_500_15	Vlan 9	N/A
	N/A		87s
101 *	Domain_L7	aabb.cc03.b999	IEEE-CFM
7	Domain_L7	Et0/0.11	
-	cust_700_17	Vlan 11	N/A



N/A  
Total Remote MEPs: 2

1s

The following example is sample output from the **show ethernet cfm mpdb** command when MEPs are configured for two Maintenance Associations (MA), MA1 and MA2, and MA2 is configured as an alias to MA1 using the **alias** command:

Device# **show ethernet cfm mpdb**

\* = Can Ping/Traceroute to MEP

```

-----
MPID  Domain Name      MacAddress      Version
Lvl   Domain ID        Ingress
Expd  MA Name            Type Id        SrvcInst
      EVC Name          Age
-----
21  *  lv13              aabb.cc00.2a03  IEEE-CFM
3    lv13              Et0/0
-    ma1               BD-V 10         1
      evc10              0s
1    *  lv13              aabb.cc00.2b02  IEEE-CFM
3    lv13              Et0/0
-    ma1               BD-V 10         1
      evc10              0s
11  *  lv13              aabb.cc00.2a02  IEEE-CFM
3    lv13              Et1/0
-    ma2 (ma1)         BD-V 20         1
      evc20              0s
1    *  lv13              aabb.cc00.2b02  IEEE-CFM
3    lv13              Et1/0
-    ma2 (ma1)         BD-V 20         1
      evc20              0s

```

Total Remote MEPs: 4



#### Note

For MPDB output, if the service is configured that matches the Continuity Check Message (CCM) MA Identifier (MAID), the output for MA Name field is "ma2 (ma1)". However, if this is a device that only has MIPs and no services are configured matching CCM MAID, the output for MA Name field is from the CCM MAID info, that is, "ma1".

The table below describes the significant fields shown in the display.

**Table 13: show ethernet cfm mpdb Field Descriptions**

Field	Description
MPID	Maintenance endpoint ID.
Domain Name	Maintenance domain name.
MacAddress	MAC address of the remote MEP.
Version	Version of the CFM protocol that is running.
Lvl	Maintenance domain level.
Domain ID	Maintenance domain identifier.

Field	Description
Ingress	Interface receiving connectivity fault management traffic.
Expd	Lifetime timer has expired.
MA Name	Name of the maintenance association.
Type Id	Identifies a port MEP, VLAN, or Bridge Domain (BD). "None" indicates an untagged port MEP and a number indicates a VLAN or BD.
SrvInst	Service instance.
EVC Name	Identifier of the Ethernet virtual circuit (EVC).
Age	Age of the message in the MIP CCDB.

**Related Commands**

Command	Description
<b>alias</b>	Configures an MA alias within a domain.
<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.

# show ethernet cfm pm

To display detailed information about Ethernet connectivity fault management (CFM) performance monitoring, use the **show ethernet cfm pm** command in privileged EXEC mode.

**show ethernet cfm pm** [**session** {*session-id*} **active**| **detail** {*session-id*} **all**}| **inactive**| **summary**}]

## Syntax Description

<b>session</b>	(Optional) Displays a performance monitoring session.
<i>session-id</i>	(Optional) Integer that identifies the session. Range is from 0 to 8000.
<b>active</b>	(Optional) Displays all active sessions.
<b>detail</b>	(Optional) Displays detailed information about the session.
<b>all</b>	(Optional) Displays detailed information about all sessions.
<b>inactive</b>	(Optional) Displays all inactive sessions.
<b>summary</b>	(Optional) Displays a summary of the current sessions.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

## Usage Guidelines

Use this command to view the CFM performance monitoring activities in your network.

## Examples

Following is sample output from the **show ethernet cfm pm** command:

```
Device# show ethernet cfm pm
-----
EPM-ID      SLA-ID      Lvl/Type/ID/Cos/Dir  Src-Mac-address  Dst-Mac-address
```

```
-----
0          3          4/BD-V/10/1/Down    2db.4980.0400    02db.4980.0200
```

Following is sample output from the **show ethernet cfm pm** command using the **session** and **summary** keywords:

```
Device# show
       ethernet cfm pm session summary
Number of Configured Session : 2
Number of Active Session: 1
Number of Inactive Session: 1
```

[show ethernet cfm pm](#), on page 393 describes the significant fields shown in each display.

**Table 14: show ethernet cfm pm Field Descriptions**

Field	Description
EPM-ID	Internal ID of the Ethernet performance monitoring session.
SLA-ID	IP SLA instance ID.
Lvl	Maintenance domain level (0 to 7).
Type	Name of the domain.
Cos	Class of service.
Dir	Direction of the MEP, either down or up.
Src-Mac-address	MAC address of the source device.
Dst-Mac-address	MAC address of the destination device.
Number of Configured Session	Number of configured performance monitoring sessions.
Number of Active Session	Number of performance monitoring sessions in the active state.
Number of Inactive Session	Number of performance monitoring sessions in the inactive state.

# show ethernet cfm smep

To display the Ethernet connectivity fault management (CFM) system maintenance endpoint (SMEP) settings on a device, use the **show ethernet cfm smep** command in privileged EXEC mode.

**Ethernet Connectivity Fault Management (CFM) Cisco Proprietary Draft 1 (CFM D1)**

**show ethernet cfm smep** [**interface gigabitethernet** *number*]

**show ethernet cfm smep** [**interface** {**gigabitethernet** *number*| **port-channel** *number*}]

## Syntax Description

<b>interface</b>	(Optional) Displays information about an interface.
<b>gigabitethernet</b> <i>number</i>	(Optional) Displays information about a Gigabit Ethernet interface. Specifies an <ul style="list-style-type: none"><li>Integer from 1 to 6 that identifies a Gigabit Ethernet interface.</li><li>Integer from 1 to 564 that identifies a port channel.</li></ul>
<b>port-channel</b> <i>number</i>	(Optional) Displays information about a configured port channel.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(33)SRD	This command was introduced.
15.0(1)XA	This command was modified. Support was added for the <b>port-channel</b> keyword.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY. The <b>port-channel</b> keyword was not supported.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

## Usage Guidelines

This command allows filtering on a per-interface basis.

Alarm Indication Signal (AIS) messages are sent by default at the configured maintenance intermediate point (MIP) level if an AIS level is not configured.

**Examples**

The following example is sample output from the **show ethernet cfm smep** command:

```
Device# show ethernet cfm smep
```

```
SMEP Settings:
```

```
-----
```

```
Interface: GigabitEthernet1/1
LCK-Status: CFM Disabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: CFM Disabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: No Defect
```

The following table describes the significant fields shown in the display.

**Table 15: show ethernet cfm smep Field Descriptions**

Field	Description
Interface	Specifies the interface type.
LCK-Status	Locked Signal function (LCK) sending status of the interface.
LCK Period	LCK transmission period on the interface.
Level to transmit LCK	Displays the level at which LCK frames are transmitted.
AIS-Status	AIS sending status of the interface.
AIS Period	AIS transmission period on the interface.
Level to transmit AIS	Displays the level at which AIS frames are transmitted.
Defect Condition	Displays the defect condition detected on the interface.

## show ethernet cfm statistics

To display Ethernet connectivity fault management (CFM) information, use the **show ethernet cfm statistics** command in privileged EXEC mode.

**show ethernet cfm statistics** [**domain** [*domain-name* [**service** {*service-instance -identifier*} **icc** *icc-code* *meg-code*] **number** *maintenance-association-number*] **vlan-id** *vlan-id*] **vpn-id** *vpn-id*] ]] **mpid** *mpid*]

### Syntax Description

<b>domain</b>	(Optional) Maintenance domain.
<i>domain-name</i>	(Optional) String of a maximum length of 154 characters.
<b>service</b>	(Optional) Maintenance association within the domain.
<i>service-instance-identifier</i>	String that identifies the service instance.
<b>icc</b>	Displays CFM information on the basis of the ITU-T Y.1731 Carrier Code (ICC)-based maintenance entity group (MEG) identifier.
<i>icc-code</i>	String that identifies the ICC. String of a maximum of six characters.
<i>meg-code</i>	String that identifies the unique MEG code. String of a maximum of 12 characters.
<b>number</b> <i>maintenance-association-number</i>	Integer from 0 to 65535 that identifies the maintenance association.
<b>vlan-id</b>	Configures a VLAN.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the VLAN.
<b>vpn-id</b>	Configures a virtual private network (VPN).
<i>vpn-id</i>	Integer from 1 to 32767 that identifies the VPN.
<b>mpid</b>	(Optional) Configures a maintenance point identifier.
<i>mpid</i>	Integer from 1 to 8191 that identifies the maintenance point.

### Command Default

All domains are displayed when none of the keywords or arguments is selected.

**Command Modes**

Privileged EXEC (#)

**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.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The <b>icc</b> keyword was added to provide support for the ICC-based MEG identifier.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

**Usage Guidelines**

Use the **show ethernet cfm statistics** command to display an overview of transmitted and received messages.

If a domain name is more than 43 characters in length, 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.

**Examples**

The following is sample output from the **show ethernet cfm statistics** command.

```
Router# show ethernet cfm statistics

BRAIN MAC: aabb.cc03.b999

DomainName: Domain_L7
MA Name: icc icc1234567890
MPID: 101
  Last clearing of counters: never
  CCMs:
    Transmitted:          242    Rcvd Seq Errors:          0
  LTRs:
    Unexpected Rcvd:          0
  LBRs:
    Transmitted:          0    Rcvd Seq Errors:          0
    Rcvd in order:        0    Rcvd Bad MSDU:          0
```

The table below describes the significant fields shown in the display.

**Table 16: show ethernet cfm statistics Field Descriptions**

Field	Description
BRAIN MAC	Bridge brain MAC address.
DomainName	Domain name.
MA Name	Maintenance association name.
MPID	Maintenance point identifier.



Field	Description
CCMs	Continuity check messages transmitted.
LTRs	Linktrace responses.
LBRs	Loopback responses.

# show ethernet cfm traceroute-cache

To display the contents of the traceroute cache, use the **show ethernet cfm trace-route cache** command in privileged EXEC mode.

**show ethernet cfm traceroute-cache** [*mac-address*] **mpid** *mpid* [**detail**] **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

<i>mac-address</i>	MAC address of the destination MEP in the format abcd.abcd.abcd.
<b>mpid</b> <i>mpid</i>	Displays a remote maintenance point. Specifies an integer from 0 to 8191 that identifies the maintenance point.
<b>detail</b>	(Optional) Displays detailed information about the traceroute cache.
<b>domain</b> <i>domain-name</i>	Displays a specific maintenance domain. String of a maximum of 154 characters in length.
<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 (#)

## 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.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SX12	This command was integrated into Cisco IOS Release 12.2(33)SX12.
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 are deprecated. You must specify the MA service via the <i>ma-fmt short-ma-name</i> identifier.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

### Usage Guidelines

Use the **show ethernet cfm traceroute-cache** command to display the contents of the traceroute cache; for example, to see the maintenance intermediate points (MIPs) and maintenance endpoints (MEPs) of a domain as they were discovered. The data is historic. The traceroute cache stores entries from previous traceroute operations.

### Examples

The following is sample output from the **show ethernet cfm traceroute-cache** command:

```
Device# show ethernet cfm traceroute-cache

Traceroute to aabb.cc00.0399 on Domain DOMAIN_PROVIDER_L5_1, Level 5, vlan 2
issued at *22:11:52.645 PST Tue Jun 21 2011
B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout
-----
      Hops      Host                MAC          Ingress      Ingr Action  Relay Action
      Forwarded Egress        Egr Action  Previous Hop
-----
! 1                aabb.cc03.b999
      Not Forwarded                                RlyHit:MEP
                                                    aabb.cc03.bb99
```

The table below describes the significant fields shown in the display.

**Table 17: show ethernet cfm traceroute-cache Field Descriptions**

Field	Description
Hops	Number of hops of the traceroute.
Host	Name of the device.
MAC	Bridge Brain MAC address of the device.
Ingress	Receiving port.
Ingr Action	Action on the ingress port: IngOk, IngFilter, IngBlocked.

Field	Description
Relay Action	Type of relay action performed: RlyNone, RlyUnknown, RlyFDB, RlyCCDB, RlyFiltered.
Forwarded	Traceroute forwarded or not forwarded.
Egress	Sending port.
Egr Action	Action on the egress port: EgrNone, EgrTTL, EgrDown, EgrBlocked, EgrOk, EgrGVRP, EgrDomainBoundary, EgrFiltered.
Previous Hop	MAC address of the neighboring device.

**Related Commands**

Command	Description
<b>clear ethernet cfm traceroute-cache</b>	Removes the contents of the traceroute cache.
<b>ethernet cfm traceroute-cache</b>	Enables caching of Ethernet CFM data learned through traceroute messages.
<b>traceroute ethernet</b>	Sends Ethernet CFM traceroute messages to a destination MAC address.

## show ethernet event microwave statistics

To display Ethernet microwave event statistics counters for one or more interfaces, use the **show ethernet event microwave statistics** command in privileged EXEC mode.

**show ethernet event microwave statistics** [*interface type number*]

### Syntax Description

<i>interface type number</i>	(Optional) Specifies the interface type and number.
------------------------------	---

### Command Modes

Privileged EXEC (#)

### Command History

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

### Usage Guidelines

If the interface is not specified, statistical counters for all interfaces are displayed.

### Examples

The following is sample output from the **show ethernet event microwave statistics** command where GigabitEthernet interface 0/0/2 has been specified:

```
Device# show ethernet event microwave statistics interface GigabitEthernet 0/0/2
```

```
Microwave Bandwidth Statistics for GigabitEthernet0/0/2
Total VSM Receive Count : 145
Total VSM Drop Count : 0
Number of transitions into Degraded state : 2
```

The table below describes the significant fields shown in the output.

**Table 18: show ethernet event microwave statistics Field Descriptions**

Field	Description
Total VSM Receive Count	Total of the bandwidth-related Vendor-Specific Messages (VSMs) received.
Total VSM Drop Count	Total of the bandwidth-related VSM dropped by the microwave transceiver.
Number of transitions into Degraded State	Number of signal degradation occurrences.

# show ethernet event microwave status

To display Ethernet microwave event status information for one or more interfaces, use the **show ethernet event microwave status** command in privileged EXEC mode.

**show ethernet event microwave status** [*interface type number*]

## Syntax Description

<i>interface type number</i>	(Optional) Specifies the interface type and number.
------------------------------	---

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

If the interface is not specified, status information for all interfaces is displayed.

## Examples

The following is sample output from the **show ethernet event microwave status** command where GigabitEthernet interface 0/0/2 has been specified:

```
Device# show ethernet event microwave status interface GigabitEthernet 0/0/2

Microwave Bandwidth Status for GigabitEthernet0/0/2
State : Degraded
Elapsed time in this state : 1:25:33
Nominal Bandwidth : 512Mbps
Current Bandwidth : 256Mbps
Lowest Bandwidth Since Entering Degraded : 64Mbps
Last VSM Received : Oct 27 14:06:19.983
Sender Transmit Period : 1 second
Sender Address : 01AB.CC00.1881
Hold Timer : Not Running
Restore Timer : Not Running
Periodic Timer : 2333 msec
Hold Time : 0 seconds
Restore Time : 10 seconds
Loss-Threshold: 3
```

The table below describes the significant fields shown in the output.

**Table 19: show ethernet event microwave status Field Descriptions**

Field	Description
State	State of the link.
Elapsed time in this state	Amount of time in the reported state

Field	Description
Nominal Bandwidth	Maximum microwave link capacity in an idle condition, in MB/s.
Current Bandwidth	Current microwave link bandwidth as reported in last Vendor-Specific message received
Lowest Bandwidth Since Entering Degraded	Lowest amount of bandwidth since the link experienced a signal degradation occurrence
Last VSM Received	Time and date of the last VSM message received
Sender Address	MAC address of the sender microwave device
Hold Timer	Indicates the state of the hold timer
Restore Timer	Indicates the state of the restore timer
Periodic Timer	Setting of the periodic timer
Hold Time	Wait-to-restore (WTR) time. Used in conjunction with the Restore Timer and Loss-Threshold fields to configure values for the hold timer, the WTR timer, and the loss threshold on the given interface.

## show ethernet lmi

To display Ethernet local management interface (LMI) Ethernet virtual connections (EVCs) configured on a device, use the **show ethernet lmi** command in privileged EXEC mode.

**show ethernet lmi** {**evc** [**detail** *evc-id* [**interface** *type number*]] | **map** **interface** *type number*] [**parameters** | **statistics**]} **interface** *type number* | **uni map** [**interface** *type number*]}

### Syntax Description

<b>evc</b>	Displays information about an EVC.
<b>detail</b>	(Optional) Displays detailed information about a specified EVC.
<i>evc-id</i>	(Optional) String of a maximum of 100 characters that identifies an EVC.
<b>interface</b>	Indicates that an interface is specified. This keyword is optional except with the <b>parameters</b> and <b>statistics</b> keywords.
<i>type</i>	String that identifies the type of interface. Valid options are the following: <ul style="list-style-type: none"> <li>• <b>ethernet</b> --Ethernet IEEE 802.3 interface</li> <li>• <b>fastethernet</b> --Fast Ethernet IEEE 802.3 interface</li> <li>• <b>gigabitethernet</b> --Gigabit Ethernet IEEE 802.3z interface</li> </ul>
<i>number</i>	Integer that identifies the interface.
<b>map</b>	(Optional) Indicates a VLAN map.
<b>parameters</b>	Displays Ethernet LMI parameters.
<b>statistics</b>	Displays Ethernet LMI statistics.
<b>uni map</b>	Displays information about the user-network interface (UNI).

### Command Modes

Privileged EXEC (#)



**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**

Use this command to check the operational statuses of EVCs.

**Examples**

The following examples show output from a **show ethernet lmi** command for interface Ethernet 0/0 using different keywords and arguments.

The following sample output is generated from the **show ethernet lmi** command using the **evc** keyword:

```
Device# show ethernet lmi evc
```

```
St   EVC Id                                     Port
-----
A   EVC_MP2MP_101                             Gi0/1
A   EVC_P2P_110                               Gi0/1
Key: St=Status, A=Active, P=Partially Active, I=Inactive, ?=Link Down
```

The following sample output is generated from the **show ethernet lmi** command using the **evc** and optional **detail** keywords:

```
Device# show ethernet lmi evc detail EVC_MP2MP_101
```

```
EVC Id: EVC_MP2MP_101
interface Ethernet0/0
  Time since Last Full Report: 00:25:25
  Ether LMI Link Status: Up
  UNI Status: Up
  UNI Id: router3-e0/0+router-e0/0
  CE-VLAN/EVC Map Type: Bundling
  VLAN: 101
  EVC Status: Active
  EVC Type: Multipoint-to-Multipoint
  Remote UNI Count: Configured = 2, Active = 2
  UNI Id                                     UNI Status   Port
  -----
  router4-e0/0+router1-e0/0                 Up            Remote
  router5-e0/0+router6-e0/0                 Up            Remote
```

The table below describes the significant fields shown in output of the **show ethernet lmi** command using the **evc** and **detail** keywords.

**Table 20: show ethernet lmi evc detail Field Descriptions**

Field	Description
EVC Id	Identifier of the EVC.
Time since Last Full Report	Number of hours, minutes, seconds since the CE requested a detailed report.
Ether LMI Link Status	Operational state of the LMI link.
UNI Status	Operational state of the UNI.
UNI Id	Identifier of the UNI between the CE and PE devices.
CE-VLAN/EVC Map Type	EVC map type: bundling, multiplex, or all-to-one
VLAN	Identifier of the VLAN.
EVC Status	Operational state of the EVC.
EVC Type	Type of connection (point-to-point or multipoint-to-multipoint).
Remote UNI Count	Number of remote UNIs that are configured and the number that are operational.
Port	Type of port, either local or remote, on which the EVC is configured. If the port is local, the interface ID is specified.

The following sample output is generated from the **show ethernet lmi** command using the **map interface** keyword:

```
Device# show ethernet lmi evc map interface Ethernet0/0
```

```
UNI Id: router3-e0/0+router-e0/0
```

```
St Evc Id CE-VLAN
```

```
-----
  A EVC_MP2MP_101      101
  A EVC_P2P_110       110
```

```
Key: St=Status, A=Active, P=Partially Active, I=Inactive, *=Default EVC,
      ?=Link Down
```

The table below describes the significant fields shown in output of the **show ethernet lmi** command using the **evc** and **map** keywords.

**Table 21: show ethernet lmi evc map Field Descriptions**

Field	Description
UNI Id	Identifier of the UNI between the CE and PE devices.

Field	Description
St	Operational state of the EVC.
Evc Id	Identifier of the EVC.
CE-VLAN	Identifier of the VLAN used by the CE.

The following sample output is generated from the **show ethernet lmi** command using the **parameters** and **interface** keywords:

```
Device# show ethernet lmi parameters interface Ethernet0/0
E-LMI Parameters for interface Ethernet0/0
  Version : MEF.16-0106
    Mode : CE
    T391 : 10
    T392 : NA
    N391 : 360
    N393 : 4
```

The table below describes the significant fields shown in output of the **show ethernet lmi** command using the **parameters** keyword.

**Table 22: show ethernet lmi parameters Field Descriptions**

Field	Description
Version	Version number of the specification that E-LMI implementation is based on.
Mode	Customer equipment or the Metro Ethernet network.
T391	Polling timer.
T392	Polling verification timer.
N391	Polling counter.
N393	Event counter.

The following sample output is generated from the **show ethernet lmi** command using the **statistics** and **interface** keywords:

```
Device# show ethernet lmi statistics interface Ethernet0/0
E-LMI Statistics for interface Ethernet0/0
  Ether LMI Link Status: Up
  UNI Status: Up
  UNI Id: router3-e0/0+router-e0/0
  Reliability Errors:
    Status Timeouts          0  Invalid Sequence Number          0
    Invalid Status Response   0  Unsolicited Status Received       0
  Protocol Errors:
    Invalid Protocol Version   0  Invalid EVC Reference Id          0
```

```

Invalid Message Type      0 Out of Sequence IE      0
Duplicated IE             0 Mandatory IE Missing    0
Invalid Mandatory IE      0 Invalid non-Mandatory IE 0
Unrecognized IE           0 Unexpected IE           0
Short Message             0
Last Full Status Enq Sent 00:50:35 Last Full Status Rcvd    00:50:35
Last Status Check Sent    00:00:06 Last Status Check Rcvd   00:00:06
Last clearing of counters 00:09:57

```

**Note**

The UNI Id field displays only when it is available from the provider edge device.

The table below describes the significant fields shown in output of the **showethernetlmi** command using the **statistics** keyword.

**Table 23: show ethernet lmi statistics Field Descriptions**

Field	Description
<b>E-LMI Statistics for interface &lt;interface-id&gt;</b>	
Ether LMI Link Status	Operational state of Ethernet LMI connectivity.
UNI Status	Operational state of the UNI.
UNI Id	Identifier of the UNI.
<b>Reliability Errors</b>	
Status Timeouts	Number of times that a status request has been sent but not received.
Invalid Sequence Number	Number of times the sequence numbers of Ethernet LMI packets do not match the sequence numbers expected.
Invalid Status Response	Number of times a status response received was invalid and discarded.
Unsolicited Status Received	Number of times status was received that had not been requested.
<b>Protocol Errors</b>	
Invalid Protocol Version	Number of times the protocol version in Ethernet LMI packets does not match what is supported.
Invalid EVC Reference Id	Number of times EVC reference IDs are invalid in Ethernet LMI packets.
Invalid Message Type	Number of message types that are not valid for LMI.

Field	Description
Out of Sequence IE	Number of information elements (IEs) that are not in the correct sequence.
Duplicated IE	Number of duplicated IEs.
Mandatory IE Missing	Number of mandatory IEs that are missing.
Invalid Mandatory IE	Number of mandatory IEs that are invalid.
Invalid non-Mandatory IE	Number of non-mandatory IEs that are invalid.
Unrecognized IE	Number of IEs that are not recognized.
Unexpected IE	Number of IEs that are unexpected.
Short Message	Number of times the Ethernet LMI message received is shorter than supported packets.
Last Full Status Enq Sent	Time in hours, minutes, and seconds when the CE sent the last full LMI status request.
Last Full Status Rcvd	Time in hours, minutes, and seconds when the CE received the last full LMI status report.
Last Status Check Sent	Time in hours, minutes, and seconds when the CE sent the last LMI status request.
Last Status Check Rcvd	Time in hours, minutes, and seconds when the CE received the last LMI status report.
Last clearing of counters	Time in hours, minutes, and seconds when the clear <b>ethernetlmi</b> command was issued for the interface.

The following sample output is generated from the **show ethernet lmi** command using the **unimap** keyword:

```
Device# show ethernet lmi uni map
```

UNI Id	EVC Id	Port
uni_sandiego	EVC_MP2MP_101	Gi0/1
uni_sandiego	EVC_P2P_110	Gi0/1

The following sample output is generated from the **show ethernet lmi** command using the **unimap** and optional **interface** keywords:

```
Device# show ethernet lmi uni map interface gigabitethernet 0/1
```

UNI Id	EVC Id	Port
uni_sandiego	EVC_MP2MP_101	Gi0/1

The table below describes the significant fields shown in output of the **showethernetlmi** command using the **unimap** keyword and **unimap** and **interface** keyword pair.

Field	Description
UNI Id	Identifier of the UNI.
EVC Id	Identifier of the EVC.
Port	Interface on the CE device.

# show ethernet loopback

To display information about the Ethernet data-plane loopback sessions on the device, use the **show ethernet loopback** command in privileged EXEC mode.

```
show ethernet loopback
{active [brief] | permitted}
[interface Ethernet interface-number]
[service instance service-instance-id]
```

## Syntax Description

<b>active</b>	Displays detailed information about the active Ethernet data-plane loopback sessions.
<i>brief</i>	(Optional) Displays brief details about the active Ethernet data-plane loopback sessions.
<b>permitted</b>	Displays the allowed service for Ethernet data-plane loopback sessions.
<b>interface Ethernet</b> <i>interface-number</i>	(Optional) Specifies the Ethernet interface on which to show the Ethernet loopback session. Valid entries range from 0 to 15.
<b>service instance</b> <i>service-instance-id</i>	(Optional) Configures the Ethernet service instance. Valid entries range from 1 to 4000.

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

Use this command to view the data-plane loopback sessions in your network.

## Examples

The following example displays an active Loopback session. The fields are self-explanatory.

```
Device# show ethernet loopback active

Loopback Session ID      : 1
Interface                 : Ethernet1/0
Service Instance          : N/A
Direction                 : Facility
Time out(sec)             : 300
```

**show ethernet loopback**

```

Status                : on
Start time            : *15:04:29.038 PST Wed Feb 29 2012
Time left             : 00:04:09
Dot1q/Dot1ad(s)      : 2
Second-dot1q(s)      : Any
Source Mac Address    : Any
Destination Mac Address : Any
Ether Type            : Any
Class of service      : Any
Llc-oui              : Any

```

The following example displays a permitted loopback session. The fields are self-explanatory.

Device# **show ethernet loopback permitted**

```

-----
Interface          SrvcInst  Direction
Dot1q(s)/Dot1ad    Second-Dot1q(s)
-----
Ethernet1/0        N/A       Terminal
3-5
Ethernet1/0        N/A       Facility
5-7,9-11,35-37,39,42
Ethernet2/0        2        Facility
1-3
Ethernet2/0        N/A       Terminal
7-10
Ethernet3/0        N/A       Terminal
13-15,17-19,100-230,400-500,10\
01-1034
Ethernet4/0        N/A       Facility
3-5

```

**Related Commands**

Command	Description
<b>ethernet loopback permit</b>	Configures an Ethernet data-plane loopback session on the interface.
<b>ethernet loopback local interface</b>	Starts and stops the Ethernet data-plane loopback session on the interface.



# show ethernet mac-tunnel engine slot

To display Ethernet MAC-in-MAC information, use the **show ethernet mac-tunnel engine slot** command in privileged EXEC mode.

**show ethernet mac-tunnel engine slot** *slot-num*

## Syntax Description

<i>slot-num</i>	Integer from 1 to 4294967295 that identifies a MAC tunnel engine slot.
-----------------	--

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

This command is used to find the B-component source address (B-SA) used in MAC-in-MAC encapsulations.

## Examples

The following is sample output from the **show ethernet mac-tunnel engine slot** command:

```
Router# show ethernet mac-tunnel engine slot 3
Tunnel-engine      B-MAC Address
0                   001d.e5e8.2274
1                   001d.e5e8.2275
```

The table below describes the significant fields shown in the display.

**Table 25: show ethernet mac-tunnel engine slot Field Descriptions**

Field	Description
Tunnel-engine	MAC tunnel identifier.
B-MAC Address	B-SA MAC address.

# show ethernet oam debug link-monitor

To display the Ethernet Operations, Administration, and Maintenance (OAM) debug link monitoring information on an interface, use the **showethernetoamdebuglink-monitor** command in privileged EXEC mode.

**show ethernet oam debug link-monitor** [*interface type number*]

## Syntax Description

<b>interface</b>	(Optional) Displays the link monitoring information on an interface.
<i>type</i>	(Optional) Displays the interface type.
<i>number</i>	(Optional) Displays the interface number.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

## Usage Guidelines

Use the **showethernetoamdebuglink-monitor** command to display Ethernet OAM debug link monitoring information on an interface.

## Examples

The following is sample output from the **showethernetoamdebuglink-monitor** command:

```
Router# show ethernet oam debug link-monitor interface gigabitEthernet 0/1
```

```
Interface Gi0/1:
first_poll = 1
symprd_tlv_sent = 0
frmprd_tlv_sent = 0
frm_poll_cnt = 1
frmsec_poll_cnt = 10
rxcrc_poll_cnt = 1
txcrc_poll_cnt = 1
symbol_period_start = never
prev_rx_error_frames = 0
total_rx_error_frames = 0
error_frame_period_start = 0
total_frame_period_start = 0
prev_error_frame_seconds = 0
total_error_frame_seconds = 0
prev_rx_crc_error_frames = 0
prev_tx_crc_error_frames = 0
total_frm_tlvs = 0
total_frmsec_tlvs = 0
```

```
total_symprd_tlvs = 0
total_frmprd_tlvs = 0
```

The table below describes the significant fields shown in the display.

**Table 26: ethernet oam debug link-monitor Field Descriptions**

Field	Description
Interface	Specifies the interface type.
first_poll	Specifies the number of counters copied in the first poll.
frmprd_tlv_sent	Specifies the number of error frame period events that are sent.
frm_poll_cnt	Specifies number of frames polled.
rxcrc_poll_cnt	Specifies the Received (RX) cyclic redundancy checks (CRCs) poll count.
txcrc_poll_cnt	Specifies the Transmitter (TX) CRCs poll count.
symbol_period_start	Specifies the symbol period start.
prev_rx_error_frames	Specifies the previous error symbol period.
total_frm_tlvs	Specifies the total number of error frames received.
total_frmsec_tlvs	Specifies the total number of frames received (in seconds ) and the type length values (TLVs) for each frame.
total_symprd_tlvs	Specifies the total symbol period and the TLVs received for each frame.
total_frmprd_tlvs	Specifies the total frame period and the TLVs received for each frame.

# show ethernet oam discovery

To display discovery information for all Ethernet operations, maintenance, and administration (OAM) interfaces or for a specific interface, use the **show ethernet oam discovery** command in privileged EXEC mode.

**show ethernet oam discovery** [*interface type number*]

## Syntax Description

<b>interface</b>	(Optional) Specifies an interface.
<i>type</i>	(Optional) Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet.
<i>number</i>	(Optional) Integer from 1 to 9 that is the number of the Ethernet interface.

## 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

This command displays the following information pertaining to Ethernet OAM discovery:

- Remote device which is directly connected to this device
- Local and remote OAM configuration and capability
- Local and remote OAM mode
- Remote platform identity
- State of the local discovery state machine

If an interface is specified, only data pertaining to the OAM peer on that interface is displayed; otherwise, data for all OAM peers (on all interfaces) is displayed.

## Examples

The following example shows output from a **show ethernet oam discovery** command for interface GigabitEthernet 6/11:

```
Device# show ethernet oam discovery interface gigabitethernet6/11

GigabitEthernet6/11
Local client
-----
  Administrative configurations:
    Mode:                active
    Unidirection:        not supported
    Link monitor:        supported (on)
    Remote loopback:     supported
    MIB retrieval:       not supported
    Mtu size:            1500
Operational status:
  Port status:          operational
  Loopback status:      no loopback
  PDU revision:         1
Remote client
-----
  MAC address: 0030.96fd.6bfa
  Vendor(oui): 0x00 0x00 0x0C (cisco)
  Administrative configurations:
    Mode:                active
    Unidirection:        not supported
    Link monitor:        supported
    Remote loopback:     supported
    MIB retrieval:       not supported
    Mtu size:            1500
```

The table below describes the significant fields shown in the display.

**Table 27: show ethernet oam discovery Field Descriptions**

Field	Description
<b>Administrative configurations</b>	
Mode	Active or passive mode of the interface
Unidirection	Operational mode
Link monitor	Status of link monitor support
Remote loopback	Status of remote loopback support
MIB retrieval	Capability of requesting MIB objects.
Mtu size	Size of the maximum transmission unit
<b>Operational status</b>	
Port status	Operational state of the port
Loopback status	Operational status of the loopback interface

Field	Description
PDU revision	Revision of the OAM configuration. A new revision results from each change to the configuration.
Remote client	
MAC address	MAC address of the remote client
Vendor (oui)	Vendor number in hexadecimal

**Related Commands**

Command	Description
<b>show ethernet oam statistics</b>	Displays detailed information about Ethernet OAM packets.
<b>show ethernet oam status</b>	Displays Ethernet OAM configurations for all interfaces or for a specific interface.
<b>show ethernet oam summary</b>	Displays active Ethernet OAM sessions.

# show ethernet oam runtime

To display Ethernet Operations, Maintenance, and Administration (OAM) runtime configurations for all interfaces or for a specific interface, use the **showethernetoamruntime** command in either user EXEC or privileged EXEC mode.

**show ethernet oam runtime interface type number**

## Syntax Description

<b>interface</b>	Specifies an interface.
<i>type number</i>	Interface type and number.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXH	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXH.

## Usage Guidelines

Use this command to display the runtime settings of link-monitoring and general OAM operations for all interfaces or for a specific interface.

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

## Examples

The following is sample output from the **showethernetoamruntime** command for Fast Ethernet interface 3/1:

```
Router# show ethernet oam runtime interface fastethernet 3/1
Runtime Settings:
-----
local_pdu: info
local_mux: fwd
local_par: fwd
local_link_status: OK
local_satisfied: No
local_stable: No
enter_loopback: No
pdu_cnt: 10
pdu_timer: Running
```

```

lost_link_timer: stopped
loopback_timer: stopped(timeout=2)
remote_state_valid: No
remote_stable: No
remote_evaluating: 0
peer version: 3
State Machine:
-----
sm(ether_oam_port Fa0/0), running yes, state ACTIVE_SEND_LOCAL

```

The table below describes the significant fields shown in the display.

**Table 28: show ethernet oam runtime Field Descriptions**

Field	Description
<b>Runtime Settings</b>	
local_pdu	Information about the number of protocol data units (PDUs) transmitted per second.
local_mux	Indicates the state of the multiplexer function of the OAM sublayer.
local_par	Indicates the state of the parser function of the OAM sublayer.
local_link_status	Status of link support.
local_satisfied	Indicates the result of comparing its local configuration and the remote configuration found in the received local information type length value (TLV) field.
local_stable	Indicates the OAM client state information in the discovery process.
pdu_cnt	Displays the count of PDUs.
pdu_timer	Time taken for PDU transmission.
lost_link_timer	Amount of time with inactivity before the link is dropped.
loopback_timer	Specified time taken by the loopback interface.
remote_state_valid	Indicates the OAM client has received remote state information.
remote_stable	Indicates remote OAM client acknowledgment of local OAM state information.
peer version	Version of the OAM peer.
State Machine	Displays information of the finite state machine.



**Related Commands**

Command	Description
<b>show ethernet oam discovery</b>	Displays discovery information for all Ethernet OAM interfaces or for a specific interface.
<b>show ethernet oam statistics</b>	Displays detailed information about Ethernet OAM packets.
<b>show ethernet oam status</b>	Displays Ethernet OAM configurations for all interfaces or for a specific interface.
<b>show ethernet oam summary</b>	Displays active Ethernet OAM sessions.

# show ethernet oam statistics

To display detailed information about Ethernet operations, maintenance, and administration (OAM) packets, use the **show ethernet oam statistics** command in privileged EXEC mode.

**show ethernet oam statistics** [*interface type number*]

## Syntax Description

<b>interface</b>	(Optional) Specifies an interface.
<i>type</i>	(Optional) Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet.
<i>number</i>	(Optional) Integer from 1 to 9 that is the number of the Ethernet interface.

## 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

Statistics that this command displays include the following:

- Rx/Tx OAM Protocol Data Unit (PDU) counters
- Link monitoring events, including event logs, if available
- Remote fault detection events
- Remote loopback events

## Examples

The following example shows output from a **showethernetoamstatistics** command for interface GigabitEthernet 6/11:

```
Device# show ethernet oam statistics interface gigabitethernet 6/11

GigabitEthernet6/11
Counters:
-----
Information OAMPDU Tx           : 9723
Information OAMPDU Rx           : 9712
Unique Event Notification OAMPDU Tx : 0
Unique Event Notification OAMPDU Rx : 0
Duplicate Event Notification OAMPDU TX : 0
Duplicate Event Notification OAMPDU RX : 0
Loopback Control OAMPDU Tx      : 0
Loopback Control OAMPDU Rx      : 0
Variable Request OAMPDU Tx      : 0
Variable Request OAMPDU Rx      : 0
Variable Response OAMPDU Tx     : 0
Variable Response OAMPDU Rx     : 0
Cisco OAMPDU Tx                 : 0
Cisco OAMPDU Rx                 : 0
Unsupported OAMPDU Tx           : 0
Unsupported OAMPDU Rx           : 0
Frames Lost due to OAM          : 0
Local event logs:
-----
0 Errored Symbol Period records
0 Errored Frame records
0 Errored Frame Period records
0 Errored Frame Second records
Remote event logs:
-----
0 Errored Symbol Period records
0 Errored Frame records
0 Errored Frame Period records
0 Errored Frame Second records
```

The table below describes the significant fields shown in the display.

**Table 29: show ethernet oam statistics Field Descriptions**

Field	Description
<b>Counters</b>	
Information OAMPDU Tx	Number of OAM PDUs transmitted
Information OAMPDU Rx	Number of OAM PDUs received
Unique Event Notification OAMPDU Tx	Number of unique event notification OAM PDUs transmitted
Unique Event Notification OAMPDU Rx	Number of unique event notification OAM PDUs received
Duplicate Event Notification OAMPDU Tx	Number of duplicate event notification OAM PDUs transmitted

Field	Description
Duplicate Event Notification OAMPDU Rx	Number of duplicate event notification OAM PDUs received
Loopback Control OAMPDU Tx	Number of loopback control OAM PDUs transmitted
Loopback Control OAMPDU Rx	Number of loopback control OAM PDUs received
Variable Request OAMPDU Tx	Number of OAM PDUs sent to request MIB objects on a remote device
Variable Request OAMPDU Rx	Number of OAM PDUs received and requesting MIB objects on a local device
Variable Response OAMPDU Tx	Number of OAM PDUs sent by the local device in response to a request from a remote device
Variable Response OAMPDU Rx	Number of OAM PDUs sent by the remote device in response to a request from a local device
Cisco OAMPDU Tx	Number of Cisco specific OAM PDUs sent
Cisco OAMPDU Rx	Number of Cisco specific OAM PDUs received
Unsupported OAMPDU Tx	Number of unsupported OAM PDUs sent
Unsupported OAMPDU Rx	Number of unsupported OAM PDUs received
Frames lost due to OAM	Number of frames discarded by the OAM client
Local event logs	Log of events on the local device
Remote event logs	Log of events on the remote device

**Related Commands**

Command	Description
<b>show ethernet oam discovery</b>	Displays discovery information for all Ethernet OAM interfaces or for a specific interface.
<b>show ethernet oam status</b>	Displays Ethernet OAM configurations for all interfaces or for a specific interface.
<b>show ethernet oam summary</b>	Displays active Ethernet OAM sessions.

# show ethernet oam status

To display Ethernet operations, maintenance, and administration (OAM) configurations for an interface, use the **show ethernet oam status** command in privileged EXEC mode.

**show ethernet oam status** [**interface** *type slot*[/*subslot*]/*port* | **vlan** *vlan*]

## Cisco ASR 901 Series Aggregation Services Router

**show ethernet oam status** [**interface** *type number*]

### Syntax Description

<b>interface</b>	(Optional) Specifies an interface.
<i>type</i>	(Optional) Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, and TenGigabitEthernet.
<i>slot</i> [/ <i>subslot</i> ]/ <i>port</i>	(Optional) Chassis slot number and port number where the Ethernet interface is located.  If the Ethernet interface is located on a shared port adapter (SPA), the subslot number may also be required. The subslot is the secondary slot number on the SPA Interface Processor (SIP) where the SPA is installed.
<b>vlan</b> <i>vlan</i>	(Optional) Limits the display to interfaces on the specified VLAN. The range is from 1 to 4094.
<i>number</i>	(Optional) Ethernet interface number. The range is from 1 to 9.

### 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.
12.2(33)SXI	This command was changed to add the optional <b>vlan</b> <i>vlan</i> keyword and argument. The <i>subslot</i> argument was added to support Ethernet interfaces located on an SPA.

Release	Modification
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 Routers.

### Usage Guidelines

Use this command to display the runtime settings of link monitoring and general OAM operations for all interfaces or for a specific interface.

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

Cisco IOS Release 12.2(33)SXI and later releases allow you to limit the display of switch port information to the specified VLAN.

### Examples

The following example shows output from the **show ethernet oam status** command for interface GigabitEthernet 0/0 when the link timeout value is specified in milliseconds (ms) using the **ethernet oam** command:

```
Device# show ethernet oam status interface gigabitethernet 0/0
GigabitEthernet0/0
General
-----
Admin state:          enabled
Mode:                 active
PDU max rate:         10 packets per second
PDU min rate:         1 packet per 2000 ms
Link timeout:         2000 milliseconds
High threshold action: no action
Link fault action:    no action
Dying gasp action:    no action
Critical event action: no action
```

The following example shows output from the **show ethernet oam status** command for interface GigabitEthernet 6/11:

```
Device# show ethernet oam status interface gigabitethernet 6/11
GigabitEthernet6/11
General
-----
Mode:                 active
PDU max rate:         10 packets per second
PDU min rate:         1 packet per 1 second
Link timeout:         5 seconds
High threshold action: no action
Link Monitoring
-----
Status: supported (on)
Symbol Period Error
  Window:              1 million symbols
  Low threshold:        1 error symbol(s)
  High threshold:       none
Frame Error
  Window:              10 x 100 milliseconds
  Low threshold:        1 error frame(s)
  High threshold:       none
Frame Period Error
  Window:              1 x 100,000 frames
  Low threshold:        1 error frame(s)
```

```

      High threshold:      none
Frame Seconds Error
      Window:             600 x 100 milliseconds
      Low threshold:      1 error second(s)
      High threshold:      none

```

The table below describes the significant fields shown in the display.

**Table 30: show ethernet oam status Field Descriptions**

Field	Description
<b>General</b>	
Mode	Active or passive mode of the interface.
PDU max rate	Maximum number of protocol data units (PDUs) transmitted per second.
PDU min rate	Minimum number of PDUs transmitted per second.
Link timeout	Amount of time with inactivity before the link is dropped.
High threshold action	Action that occurs when the high threshold for an error is exceeded.
<b>Link Monitoring</b>	
Status	Operational state of the port.
<b>Symbol Period Error</b>	
Window	Specified number of error symbols.
Low threshold	Minimum number of error symbols.
High threshold	Maximum number of error symbols.
<b>Frame Error</b>	
Window	Specified amount of time, in milliseconds.
Low threshold	Minimum number of error frames.
High threshold	Maximum number of error frames.
<b>Frame Period Error</b>	
Window	Frequency at which the measurement is taken, in milliseconds.
Low threshold	Minimum number of error frames.

Field	Description
High threshold	Maximum number of error frames.
<b>Frame Seconds Error</b>	
Window	Frequency at which the measurement is taken, in milliseconds.
Low threshold	Lowest value at which an event will be triggered.
High threshold	Highest value at which an event will be triggered.

**Related Commands**

Command	Description
<b>show ethernet oam discovery</b>	Displays discovery information for all Ethernet OAM interfaces or for a specific interface.
<b>show ethernet oam statistics</b>	Displays detailed information about Ethernet OAM packets.
<b>show ethernet oam summary</b>	Displays active Ethernet OAM sessions.



# show ethernet oam summary

To display active Ethernet operations, maintenance, and administration (OAM) sessions on a device, use the **show ethernet oam summary** command in privileged EXEC mode.

**show ethernet oam summary**

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

**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.

**Examples** The following example shows output from a **show ethernet oam summary** command:

Device# **show ethernet oam summary**

Symbols: \* - Master Loopback State, # - Slave Loopback State  
 Capability codes: L - Link Monitor, R - Remote Loopback  
 U - Unidirection, V - Variable Retrieval

Local Interface	MAC Address	Remote Vendor	Mode	Capability
Fa3/1	0080.09ff.e4a0	00000C	active	L R
Gi6/11	0030.96fd.6bfa	00000C	active	L R

The table below describes the significant fields shown in the display.

**Table 31: show ethernet oam summary Field Descriptions**

Field	Description
Local Interface	Type of local interface
MAC Address	MAC address of the local interface
Remote Vendor	The vendor for the remote device.

Field	Description
Mode	Operational state of the remote interface
Capability	Functions the local interface can perform

**Related Commands**

Command	Description
<b>show ethernet oam discovery</b>	Displays discovery information for all Ethernet OAM interfaces or for a specific interface.
<b>show ethernet oam status</b>	Displays Ethernet OAM configurations for all interfaces or for a specific interface.
<b>show ethernet oam statistics</b>	Displays detailed information about Ethernet OAM packets.

## show ethernet ring g8032 brief

To display a brief description of the functional state of the Ethernet Ring Protection (ERP) instance, use the **show ethernet ring g8032 brief** command in privileged EXEC mode.

**show ethernet ring g8032 brief** [*ring-name* [**instance** *instance-id*]]

### Syntax Description

<i>ring-name</i>	(Optional) Ethernet ring name.
<b>instance</b> <i>instance-id</i>	(Optional) Enter the <b>instance</b> keyword followed by the instance identifier. The instance identifier is either 1 or 2.

### Command Modes

Privileged EXEC (#)

### 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.

### Usage Guidelines

This command can be used to display status information for all ERP instances in an ERP ring, for an ERP instance for a specified ERP ring, or for all ERP instances configured on the device.

The information displayed in the output includes the following:

- The Ethernet ring name
- The instance number
- The node type
- The node state
- Each of the interfaces (Port0 and Port1) and their respective states for handling data traffic (as shown in the legend of the output)

### Examples

The following is sample output from the **show ethernet ring g8032 brief** command. The fields shown in the display are self-explanatory.

```
Device# show ethernet ring g8032 brief
```

```
R: Interface is the RPL-link
F: Interface is faulty
B: Interface is blocked
```

show ethernet ring g8032 brief

FS: Local forced switch  
MS: Local manual switch

RingName	Inst	NodeType	NodeState	Port0	Port1
-----					
abc	1	Normal	Pending	B	

# show ethernet ring g8032 configuration

To display the Ethernet Ring Protection (ERP) switching configuration, use the **show ethernet ring g8032 configuration** command in privileged EXEC mode.

**show ethernet ring g8032 configuration** [*ring-name*] [*instance instance-id*]

## Syntax Description

<i>ring-name</i>	(Optional) Ethernet ring name.
<b>instance</b> <i>instance-id</i>	(Optional) Enter the <b>instance</b> keyword followed by the instance identifier. The instance identifier is either 1 or 2.

## Command Modes

Privileged EXEC (#)

## 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.

## Usage Guidelines

This command displays the output of the Ethernet ring instance configuration manager. Refer to the output to verify whether the configuration is valid and to identify any incomplete or omitted parameters.

## Examples

The following is sample output from the **show ethernet ring g8032 configuration** command.

```
Device# show ethernet ring g8032 configuration

ethernet ring ring0
Port0: GigabitEthernet0/0/0 (Monitor: GigabitEthernet0/0/0)
Port1: GigabitEthernet0/0/4 (Monitor: GigabitEthernet0/0/4)
Exclusion-list VLAN IDs: 4001-4050
Open-ring: no
Instance 1
  Description:
  Profile:    opp
  RPL:
  Inclusion-list VLAN IDs: 2,10-500
  APS channel
  Level: 7
  Port0: Service Instance 1
  Port1: Service Instance 1
  State: configuration resolved
```

The table below describes the significant fields shown in the display.

**Table 32: show ethernet ring g8032 configuration Field Descriptions**

Field	Description
ethernet ring	Ethernet ring number
Exclusion-list VLAN IDs	List of unprotected VLANs
Open-ring	Identifies whether the Ethernet ring is configured as an open ring
Instance	Instance identifier
Inclusion-list VLAN IDS	List of protected VLANs
State	State of the ERP protection switching configuration

## show ethernet ring g8032 port status

To display Ethernet ring port status information for the interface, use the **show ethernet ring g8032 port status** command in privileged EXEC mode.

**show ethernet ring g8032 port status interface *type number***

### Syntax Description

<b>interfacetype number</b>	Interface type and number. Enter the <b>interface</b> keyword followed by the interface type and interface number.
-----------------------------	--

### Command Modes

Privileged EXEC (#)

### 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.

### Usage Guidelines

The display includes the list of VLANs that are blocked or unblocked and the state of the instance on the port. An instance can also be blocked or unblocked.

### Examples

The following is sample output from the **show ethernet ring g8032 port status** command. The fields shown in the display are self-explanatory.

```
Device# show ethernet ring g8032 port status interface gigabitethernet 0/0
```

```
Port: GigabitEthernet0/0
Ring: ring0
    Block vlan list: 3,501-1000
    Unblock vlan list: 2,10-500
    REQ/ACK: 5/5
    Instance 1 is in Unblocked state
```

```
Port: GigabitEthernet0/0
Ring: ring0
    Block vlan list: 3,501-1000
    Unblock vlan list: 2,10-500
    REQ/ACK: 6/6
    Instance 1 is in Unblocked state
```

# show ethernet ring g8032 profile

To display the settings for one or more Ethernet ring profiles, use the **show ethernet ring g8032 profile** command in privileged EXEC mode.

**show ethernet ring g8032 profile** [*profile-name*]

## Syntax Description

<i>profile-name</i>	(Optional) Displays the settings for the specified profile. If the profile name is not specified, the settings for all profiles are displayed.
---------------------	--

## Command Modes

Privileged EXEC (#)

## 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.

## Examples

The following is sample output from the **show ethernet ring g8032 profile** command. The fields shown in the display are self-explanatory.

```
Device# show ethernet ring g8032 profile ERP-profile
Ethernet ring profile name: ERP-profile
  WTR interval: 1 minutes
  Guard interval: 500 milliseconds
  Hold-off interval: 0 seconds
  Non-revertive mode
```



## show ethernet ring g8032 statistics

To display the number of events and Ring Automatic Protection Switching (R-APS) messages received for an Ethernet Ring Protocol (ERP) instance, use the **show ethernet ring g8032 statistics** command in privileged EXEC mode.

**show ethernet ring g8032 statistics** [*ring-name* [**instance** *instance-id*]]

### Syntax Description

<i>ring-name</i>	(Optional) Ethernet ring name.
<b>instance</b> <i>instance-id</i>	(Optional) Enter the <b>instance</b> keyword followed by the instance identifier. The instance identifier is either 1 or 2.

### Command Modes

Privileged EXEC (#)

### 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.

### Usage Guidelines

This command can be used to display the number of events and R-APS messages received for all ERP instances in an ERP ring, for an ERP instance for a specified ERP ring, or for all ERP instances configured on the router.

### Examples

The following is sample output from the **show ethernet ring g8032 statistics** command.

```
Device# show ethernet ring g8032 statistics RingA instance 1

Statistics for Ethernet ring RingA instance 1
Local SF detected:
  Port0: 1
  Port1: 0
R-APS      Port0 (Tx/Rx)  Port1 (Tx/Rx)
-----
NR       : 1/1      1/1
NR, RB   : 0/1      0/1
SF       : 1/0      1/0
MS       : 0/0      0/0
FS       : 0/0      0/0
```

The table below describes the significant fields shown in the display.

**Table 33: show ethernet ring g8032 statistics Field Descriptions**

Field	Description
NR	No request R-APS message.
RB	Route blocked R-APS message.
SF	Signal failure event.
MS	Manual switch event.
FS	Force switch event.

## show ethernet ring g8032 status

To display a status summary for the Ethernet Ring Protection (ERP) instance, use the **show ethernet ring g8032 status** command in privileged EXEC mode.

**show ethernet ring g8032 status** [*ring-name* [**instance** *instance-id*]]

### Syntax Description

<i>ring-name</i>	(Optional) Ethernet ring name.
<b>instance</b> <i>instance-id</i>	(Optional) Enter the <b>instance</b> keyword followed by the instance identifier. The instance identifier is either 1 or 2.

### Command Modes

Privileged EXEC (#)

### 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.

### Usage Guidelines

This command can be used to display status information for all ERP instances in an ERP ring, for an ERP instance for a specified ERP ring, or for all ERP instances configured on the device.

The information displayed in the output includes the following:

- The G.8032 node type and state
- Each of the interfaces and whether any interface is the Ring Protection Link (RPL)
- Whether a fault has been detected on the interface
- Whether the interface has been blocked
- The configured profile for the instance

### Examples

The following are examples of output from the **show ethernet ring g8032 status** command for Ethernet RingA (instances 1 and 2), and Ethernet Ring B, (instance 1). Note that for Ring B, instance 1, an ERP profile has not been configured. Therefore, the default ERP profile values are used.

```
Device# show ethernet ring g8032 status RingA instance 1

Ethernet ring RingA instance 1 is Normal node in Protection state
  Port0: GigabitEthernet0/0/1 (Monitor: GigabitEthernet0/0/1)
  APS-Channel: Service Instance 1
```

```

        Status: NonRPL, faulty, blocked
        Remote R-APS NodeId: 0022.bddd.ff99, BPR: 0
Port1: GigabitEthernet1/1/1 (Monitor: GigabitEthernet1/1/1)
        APS-Channel: Service Instance 1
        Status: NonRPL
        Remote R-APS NodeId: 0022.bddd.ff99, BPR: 0
APS Level: 3
Profile: ERP-profile
        WTR interval: 60s
        Guard interval: 100ms
        Hold-off interval: 1s
        Revertive mode

Device# show ethernet ring g8032 status RingA instance 2

Ethernet ring RingA instance 2 is RPL Owner node in Idle state
Port0: GigabitEthernet0/0/0
        Monitor: GigabitEthernet0/0/0
        APS-Channel: vlan 1
        Status: NonRPL
        Remote R-APS NodeId: 0022.bddd.ff99, BPR: 0
Port1: GigabitEthernet1/1/1
        Monitor: GigabitEthernet1/1/1
        APS-Channel: vlan 1
        Status: RPL, blocked
        Remote R-APS NodeId: 0022.bddd.ff99, BPR: 0
APS Level: 3
Profile: ERP-profile
        WTR interval: 60s
        Guard interval: 100ms
        Hold-off interval: 1s
        Revertive mode

Device# show ethernet ring g8032 status RingB instance 1

Ethernet ring RingB instance 1 is RPL Owner node in ForcedSwitch state
Port0: GigabitEthernet0/0/2 (Monitor: GigabitEthernet0/0/2)
        APS-Channel: vlan 1
        Status: NonRPL, local fs, blocked
        Remote R-APS NodeId: 0022.bddd.ff99, BPR: 0
Port1: GigabitEthernet1/1/2
        Monitor: GigabitEthernet1/1/2
        APS-Channel: vlan 1
        Status: RPL
        Remote R-APS NodeId: 0022.bddd.ff99, BPR: 0
APS Level: 3
Open-ring topology
Version 1 compatible
Profile: (not configured)
        WTR interval: 300s
        Guard interval: 500ms
        Hold-off interval: 0s
        Revertive mode

```

The table below describes the significant fields shown in the display.

**Table 34: show ethernet ring g8032 status Field Descriptions**

Field	Description
Ethernet ring	Ethernet ring number.
Open-ring	Identifies whether the Ethernet ring is configured as an open ring.
Instance	Instance identifier.
State	State of the ERP protection switching configuration.



# show ethernet ring g8032 summary

To display a summary of the number of Ethernet Ring Protocol (ERP) instances in each state of the ERP switching process, use the **show ethernet ring g8032 summary** command in privileged EXEC mode.

**show ethernet ring g8032 summary**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## 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.

## Examples

The following is sample output from the **show ethernet ring g8032 summary** command.

```
Device# show ethernet ring g8032 summary
```

```
Chassis  NodeId: 88f0.7768.1a99
States
```

```
-----
Idle           3
Manual Switch  0
Forced Switch  0
Protection     8
Pending        0
-----
Total          11
```

The table below describes the significant fields shown in the display.

**Table 35: show ethernet ring g8032 summary Field Descriptions**

Field	Description
Idle	No failure or administrative condition exists.
Manual switch	Manual switch condition exists.
Forced switch	Force switch condition exists.
Protection	Protection state.
Pending	Pending state.



# show ethernet ring g8032 trace

To display information about Ethernet Ring Protection (ERP) traces, use the **show ethernet ring g8032 trace** command in privileged EXEC mode.

**show ethernet ring g8032 trace**{**ctrl** [*ring-name* **instance** *instance-id*]| **sm**}

## Syntax Description

<b>ctrl</b>	Displays Ethernet ring controller traces.
<i>ring-name</i>	(Optional) Ethernet ring name.
<b>instance</b> <i>instance-id</i>	(Optional) Enter the <b>instance</b> keyword followed by the Ethernet ring instance number.
<b>sm</b>	Displays Ethernet ring state machine traces.

## Command Modes

Privileged EXEC (#)

## 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.

## Examples

The following example shows how to enable the **show ethernet ring g8032 trace** command. Output is generated only when ERP trace information is available.

```
Device# show ethernet ring g8032 trace sm
```



# show ethernet service dynamic

To display information about Layer 2 context service instances, use the **show ethernet service dynamic** command in privileged EXEC mode.

**show ethernet service dynamic** [*id identifier interface type number*] [**detail**]

## Syntax Description

<b>id identifier</b>	(Optional) Specifies the Layer 2 context service instance identifier.
<b>interface</b>	(Optional) Declares a specific interface selection for a specified Layer 2 context service instance.
<b>type</b>	(Optional) Type of interface
<b>number</b>	(Optional) Number of the interface.
<b>detail</b>	(Optional) Displays detailed information about Layer 2 context service instances or about a specific Layer 2 context service instance.

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

This command is useful for system monitoring and troubleshooting.

## Examples

The following is sample output from the **show ethernet service dynamic** command:

```
Router# show ethernet service dynamic
Identifier  Type      Interface          State    CE-Vlans
1           L2CXT     GigabitEthernet2/2 Down

L2Context 1 does not have any dynamically created service instance
1           L2CXT     GigabitEthernet2/15 Up

Total number of Dynamic Service Instances under L2context(1) = 1
1           Dynamic   GigabitEthernet2/15 Up
The table below describes the significant fields shown in the display.
```

**Table 36: show ethernet service dynamic Field Descriptions**

Field	Description
Identifier	Service instance identifier.
Type	Type of service instance.
Interface	Interface type and number with which the service instance is associated.
State	State of the interface.
CE-Vlans	Customer edge (CE) device VLAN ID.

The following example displays various types of service instances under an interface with a specific instance ID:

```
Router# show ethernet service dynamic 23 interface ethernet 0/0 detail
Service Instance ID: 1
Service instance type: L2Context
Initiators: unclassified vlan
Control policy: policy1
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 200-300 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In   Bytes In   Pkts Out   Bytes Out
    0      0         0         0
```

The table that follows describes the significant fields shown in the display.

**Table 37: show ethernet service dynamic Field Descriptions**

Field	Description
Service Instance ID	Service instance identifier.
Service instance type	Service instance type
Initiators	Service initiators associated with the L2 context.
Control Policy	Control policy associated with the L2 context service instance.
Associated Interface	CE device VLAN ID.
Associated EVC	Ethernet virtual circuits (EVCs) associated with a device.

Field	Description
L2protocol drop	Number of Layer 2 protocol packet data units (PDUs) dropped.
CE-Vlans	VLANs associated with a device.
Encapsulation	Type of encapsulation used to enable session-level traffic classification.
Interface	Interface type and number with which the service instance is associated.
State	State of the interface.
EFP Statistics	Statistics of the Layer 2 service instances.

#### Related Commands

Command	Description
<b>clear ethernet service instance</b>	Clears Ethernet service instance attributes such as MAC addresses and statistics, and purges Ethernet service instance errors.
<b>show ethernet service instance</b>	Displays information about Ethernet service instances.
<b>show ethernet service interface</b>	Displays interface-only information about Ethernet customer service instances.

# show ethernet service evc

To display information about Ethernet virtual connections (EVCs), use the **showethernetserviceevc** command in privileged EXEC mode.

**show ethernet service evc**[**detail** | **id** *evc-id* [**detail**] | **interface** *type* *number* [**detail**]]

## Syntax Description

<b>interface detail</b>	(Optional) Displays detailed information about service instances or the specified service instance ID or interface.
<b>id</b>	(Optional) Displays EVC information for the specified service.
<i>evc-id</i>	(Optional) String from 1 to 100 characters that identifies the EVC.
<b>interface</b>	(Optional) Displays service instance information for the specified interface.
<i>type</i>	(Optional) Type of interface.
<i>number</i>	(Optional) Number of the interface.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(25)SEG	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 Cisco ASR 901 Series Aggregation Services Routers.

## Usage Guidelines

This command is useful for system monitoring and troubleshooting.

## Examples

Following is sample output from the **show ethernet service evc** command:

Device# **show ethernet service evc**

```

Identifier                Type  Act-UNI-cnt  Status
BLUE                      P-P    2           Active
PINK                      MP-MP   2           PartiallyActive
PURPLE                    P-P    2           Active
BROWN                     MP-MP   2           Active
GREEN                     P-P    3           Active
YELLOW                    MP-MP   2           PartiallyActive
BANANAS                   P-P    0           InActive
TEST2                     P-P    0           NotDefined
ORANGE                    P-P    2           Active
TEAL                      P-P    0           InActive

```

The table below describes the significant fields in the output.

**Table 38: show ethernet service evc Field Descriptions**

Field	Description
Identifier	EVC identifier.
Type	Type of connection, for example point-to-point (P-P) or multipoint-to-multipoint (MP-MP).
Act-UNI-cnt	Number of active user network interfaces (UNIs).
Status	Availability status of the EVC.

## Related Commands

Command	Description
<b>show ethernet instance</b>	Displays information about Ethernet customer service instances.
<b>show ethernet interface</b>	Displays interface-only information about Ethernet customer service instances.

## show ethernet service instance

To display information about Ethernet service instances, use the **show ethernet service instance** command in privileged EXEC mode.

**show ethernet service instance** [**detail**] **id** *id* {**interface** *type number* [**detail**] **mac** {**security** [**address** | **last violation** | **statistics**] | **static address**} | **load-balance** | **mac-tunnel** [**detail**] } | **platform** | **stats** | **interface** *type number* [**detail** | **load-balance** | **platform** | **stats** | **summary**] | **mac security** [**address** | **last violation** | **statistics**] | **platform** | **policy-map** | **stats** | **summary**]

### Cisco ASR 901 Series Aggregation Services Router

**show ethernet service instance** [**detail**] **id** *id* **interface** *type number* [**detail**] **mac security** [**address** | **last violation** | **statistics**] | **platform** | **stats**] | **interface** *type number* [**detail**] **platform** | **stats** | **summary**] | **mac security** [**address** | **last violation** | **statistics**] | **platform** | **policy-map** | **stats** | **summary**]

#### Syntax Description

<b>detail</b>	(Optional) Displays detailed information about service instances, a specific service instance, or about a MAC tunnel service instance.
<b>id</b>	(Optional) Displays a specific service instance on an interface that does not map to a VLAN.
<i>id</i>	(Optional) Integer from 1 to 4294967295 that identifies a service instance on an interface that does not map to a VLAN.
<b>interface</b>	(Optional) Declares a specific interface selection for a specified service instance.
<i>type</i>	(Optional) Type of interface.
<i>number</i>	(Optional) Number of the interface.
<b>mac</b>	(Optional) Displays MAC address data.
<b>security</b>	(Optional) Displays the MAC security status of a specified service instance.
<b>address</b>	(Optional) Displays the secure addresses on the specified service instance.
<b>last violation</b>	(Optional) Displays the last violation recorded on the specified service instance.
<b>statistics</b>	(Optional) Displays MAC security statistics for the specified service instance.

<b>static</b>	(Optional) Displays MAC static address information.
<b>address</b>	(Optional) Displays MAC static addresses in a bridge domain.
<b>load-balance</b>	(Optional) Displays EtherChannel load-balancing information.
<b>mac-tunnel</b>	(Optional) Displays the MAC tunnel Ethernet service instance identifier.
<b>platform</b>	(Optional) Displays platform information for a specified service instance.
<b>stats</b>	(Optional) Displays statistics for a specified service instance.
<b>summary</b>	(Optional) Displays summary information about service instances.
<b>policy-map</b>	(Optional) Displays the policy map for service instances.
<b>mac security</b>	(Optional) Displays the MAC security status of the specified service instance for Cisco ASR 901 Series Aggregation Services Routers.

**Command Modes**

Privileged EXEC (#)

**Command History**

<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.
12.2(33)SRD	This command was modified. The <b>address</b> , <b>detail</b> , <b>lastviolation</b> , <b>macsecurity</b> , <b>platform</b> , <b>statistics</b> , <b>stats</b> , and <b>summary</b> keywords were added.
12.2(33)SRE	This command was modified. The <b>address</b> , <b>mac-tunnel</b> , and <b>static</b> keywords were added.
15.0(1)S	This command was modified. The <b>load-balance</b> keyword was added.
15.1(2)S	This command was modified. The output was extended to include information about Layer 2 context service instances, service initiators associated with a Layer 2 context, and the control policy associated with a Layer 2 context service instance.

Release	Modification
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S to provide support for the Cisco ASR 903 Router. This command was modified to provide support for Ethernet Flow Points (EFPs) on trunk ports (interfaces). The output includes information about trunk ports, if applicable.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

This command is useful for system monitoring and troubleshooting.

### Examples

The following is sample output from the **show ethernet service instance** command:

```
Device# show ethernet service instance
```

```
Identifier  Type      Interface      State      CE-Vlans
4           static    GigabitEthernet3/2  Down
```

The table that follows describes the significant fields shown in the display.

**Table 39: show ethernet service instance Field Descriptions**

Field	Description
Identifier	Service instance identifier.
Type	Service instance type, as applicable, such as Static, L2Context, Dynamic, or Trunk.
Interface	Interface type and number with which the service instance is associated.
State	Service instance operational status such as Up, Down, or AdminDown.
CE-Vlans	Customer edge (CE) device VLAN ID.

Following is sample output from the **show ethernet service instance detail** command. The output shows details of different service instances configured on a given platform.

```
Device# show ethernet service instance detail
```

```
Service Instance ID: 1
Service instance type: L2Context
Initiators: unclassified vlan
Control policy: ABC
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans:
```



```

Encapsulation: dot1q 200-300 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In   Bytes In   Pkts Out  Bytes Out
    0       0         0         0

Service Instance ID: 2
Service instance type: Dynamic

Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans: 10-20
Encapsulation: dot1q 201 vlan protocol type 0x8100

```

```

Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In   Bytes In   Pkts Out  Bytes Out
    0       0         0         0

```

Following is sample output from the **show ethernet service instance interface detail** command. The output shows details of service instances configured on a specific interface.

Device# **show ethernet service instance interface ethernet 0/0 detail**

```

Service Instance ID: 1
Service instance type: L2Context
Initiators: unclassified vlan
Control policy: ABC
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 200-300 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In   Bytes In   Pkts Out  Bytes Out
    0       0         0         0

Service Instance ID: 2
Service instance type: Dynamic

Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans: 10-20
Encapsulation: dot1q 201 vlan protocol type 0x8100

Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In   Bytes In   Pkts Out  Bytes Out
    0       0         0         0

Service Instance ID: 3
Service instance type: static
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans: 10-20
Encapsulation: dot1q 201 vlan protocol type 0x8100

Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In   Bytes In   Pkts Out  Bytes Out
    0       0         0         0

```

Following is sample output from the **show ethernet service instance id interface detail** command. The output shows details of a specific service instance configured on an interface.

```
Device# show ethernet service instance id 1 interface ethernet 0/0 detail
```

```
Service Instance ID: 1
Service instance type: L2Context
Initiators: unclassified vlan
Control policy: ABC
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 200-300 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In   Bytes In   Pkts Out  Bytes Out
    0         0         0         0
```

This is an example of output from the **show ethernet service instance detail** command on a Cisco ASR 901 Series Aggregation Services Router:

```
Device# show ethernet service instance id 1 interface gigabitEthernet 0/1 detail
```

```
Service Instance ID: 1
Associated Interface: GigabitEthernet0/13
Associated EVC: EVC_P2P_10
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 10 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In Bytes In Pkts Out Bytes Out
  214 15408 97150 6994800
EFP Microblocks:
*****
Microblock type: Bridge-domain
Bridge-domain: 10
```

This is an example of output from the **show ethernet service instance stats** command on a Cisco ASR 901 Series Aggregation Services Router:

```
Device# show ethernet service instance id 1 interface gigabitEthernet 0/13 stats
```

```
Service Instance 1, Interface GigabitEthernet0/13
Pkts In Bytes In Pkts Out Bytes Out
214 15408 97150 6994800
```

**Table 40: show ethernet service instance Field Descriptions**

Field	Description
Service Instance ID	Service instance identifier.
Service instance type	Type of service instance.
Initiators	Service initiators associated with the service instance.
Control Policy	Control policy associated with the service instance.
Associated Interface	Interface on which the service instance is configured.

Field	Description
Associated EVC	Ethernet virtual circuit (EVC) associated with a device.
L2protocol drop	Number of Layer 2 protocol data units (PDUs) dropped.
CE-Vlans	VLANs associated with a device.
Encapsulation	Type of encapsulation used to enable session-level traffic classification.
Interface	Interface type and number with which the service instance is associated.
State	Up or Down.
EFP Statistics	Traffic on the service instance.

### Related Commands

Command	Description
<b>clear ethernet service instance</b>	Clears Ethernet service instance attributes such as MAC addresses and statistics and purges Ethernet service instance errors.
<b>show ethernet service interface</b>	Displays interface-only information about Ethernet customer service instances.

# show ethernet service interface

To display interface-only information about Ethernet customer service instances for all interfaces or for a specified interface, use the **show ethernet service interface** command in privileged EXEC mode.

**show ethernet service interface** [*type number*] [**detail**]

## Syntax Description

<i>type</i>	(Optional) Type of interface.
<i>number</i>	(Optional) Number of the interface.
<b>detail</b>	(Optional) Displays detailed information about all interfaces or a specified service instance ID or interface.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(25)SEG	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S to provide support for the Cisco ASR 903 Device. This command was modified to provide support for Ethernet Flow Points (EFPs) on trunk ports (interfaces). The output includes information about trunk ports, if applicable.
Cisco IOS XE Release 3.6S	This command was modified. The output was modified to display the number of the bridge domains associated with the EFPs on an interface, if applicable.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain “Output” are displayed.

## Examples

The following is an example of output from the **show ethernet service interface** command when the **detail** keyword is specified:

```
Device# show ethernet service interface detail
```

```

Interface: FastEthernet0/1
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/2
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/3
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Bridge-Domains: 10,20,30
<output truncated>
Interface: GigabitEthernet0/1
ID: PE2-G101
CE-VLANS: 10,20,30
EVC Map Type: Bundling-Multiplexing
Associated EVCs:
EVC-ID CE-VLAN
WHITE 30
RED 20
BLUE 10
Associated Service Instances:
Service-Instance-ID CE-VLAN
10 10
20 20
30 30

```

The table below describes the significant fields in the output.

**Table 41: show ethernet service interface Field Descriptions**

Field	Description
Interface	Interface type and number.
Identifier	EVC identifier.
ID	EVC identifier.
CE-VLANS	VLANs associated with the customer edge (CE) device.
EVC Map Type	UNI service type; for example, Bundling, Multiplexing, All-to-one Bundling.
Bridge-Domains	Bridge domains associated with the EFPs on the interface.
Associated EVCs	EVCs associated with a device.
EVC-ID CE-VLAN	EVC identifier and associated VLAN.
Associated Service Instances	Service instances associated with a device.
Service-Instance-ID CE-VLAN	Service instance identifier and its associated CE VLAN.

**Related Commands**

Command	Description
<b>service instance ethernet</b>	Defines an Ethernet service instance and enters Ethernet service configuration mode.
<b>show ethernet evc</b>	Displays information about Ethernet customer service instances.
<b>show ethernet interface</b>	Displays interface-only information about Ethernet customer service instances.

# show ethernet service mac-tunnel

To display information about MAC tunnels, use the **showethernetservicemac-tunnel** command in privileged EXEC mode.

**show ethernet service mac-tunnel** {*id* [*detail*]| *summary*}

## Syntax Description

<i>id</i>	Integer from 1 to 2147483647 that identifies a MAC-in-MAC tunnel.
<b>detail</b>	Displays detailed information about a MAC-in-MAC tunnel.
<i>summary</i>	Displays summary information about a MAC-in-MAC tunnel.

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

This command is useful for system monitoring and troubleshooting.

## Examples

The following is sample output of the **showethernetservicemac-tunnel** command:

```
Router# show ethernet service mac-tunnel 1 detail tunnel id 1
State: Up
EFP Microblocks:
*****
Microblock type: Bridge-domain
Bridge-domain: 10
No. of Service Instances: 1
Service Instance ID: 1
Associated Tunnel Id: 1
Encapsulation: dot1ah 1 vlan-type 0x88E7
State: Up
Mac-flush: MIRP enabled/MIRP cos 7
EFP Microblocks:
*****
Microblock type: Bridge-domain
Bridge-domain: 1 c-mac
The table below describes the significant fields shown in the display.
```

**Table 42: show ethernet service mac-tunnel detail Field Descriptions**

Field	Description
State	Operational state of the MAC tunnel.
EFP Microblocks	Mechanism for external components to store information in the EFP structure.
Microblock type	Type of microblock. In this case, bridge domain is the microblock.
No. of Service Instances	Number of service instances configured under the MAC tunnel.
Service Instance ID	Service instance identifier.
Associated Tunnel Id	ID of the MAC tunnel under which the service instance is configured.
Encapsulation	Type of encapsulation used for the service instance.
Mac-flush	Type of remote MAC address flush mechanism that is currently supported. In this case, it is Multiple I-SID Registration Protocol (MIRP).
Bridge-domain: 1 c-mac	Type of bridge domain configured.

Router# **show ethernet service mac-tunnel summary**

```

Total      Up    AdminDo    Down    ErrorDi    Unknown    Deleted    BdAdmDo
bdomain    1      1          0        0          0          0          0
other      0      0          0        0          0          0          0
Associated Tunnel Id: 1
Total      Up    AdminDo    Down    ErrorDi    Unknown    Deleted    BdAdmDo
bdomain    1      1          0        0          0          0          0
other      0      0          0        0          0          0          0

```

The table below describes the significant fields shown in the display.

**Table 43: show ethernet service mac-tunnel summary Field Descriptions**

Field	Description
Total	Total number of bridge domains or other forwarding mechanisms configured.
Up	Number of bridge domains or other forwarding mechanisms that are operational.
AdminDo	Number of bridge domains or other forwarding mechanisms that are administratively shut down.



Field	Description
Down	Number of bridge domains or other forwarding mechanisms that are not operational.
ErrorDi	Number of bridge domains or other forwarding mechanisms that are disabled.
Unknown	Number of bridge domains or other forwarding mechanisms for which operational status is unknown.
Deleted	Number of configurations removed.
BdAdmDo	Indicates that the bridge domain was shut down.
bdomain	Bridge domain.
other	Any forwarding mechanism other than a bridge domain.
Associated Tunnel Id	ID of the MAC tunnel under which the service instance is configured.

# show lacp

To display Link Aggregation Control Protocol (LACP) and multi-chassis LACP (mLACP) information, use the **show lacp** command in either user EXEC or privileged EXEC mode.

**show lacp** {*channel-group-number* {**counters**| **internal** [**detail**] | **neighbor** [**detail**] } | **multi-chassis** [**load-balance**] {**group** *number* | **port-channel** *number* } | **sys-id**}

## Cisco ASR 901 Series Aggregation Services Router

**show lacp** {*channel-group-number* {**counters**| **internal** [**detail**] | **neighbor** [**detail**] | **sys-id** } }

### Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The following are valid values: <ul style="list-style-type: none"> <li>• Cisco IOS 12.2 SB and Cisco IOS XE 2.4 Releases--from 1 to 64</li> <li>• Cisco IOS 12.2 SR Releases--from 1 to 308</li> <li>• Cisco IOS 12.2 SX Releases--from 1 to 496</li> <li>• Cisco IOS 15.1S Releases—from 1 to 564</li> <li>• Cisco ASR 901 Series Aggregation Services Router—from 1 to 8</li> </ul>
<b>counters</b>	Displays information about the LACP traffic statistics.
<b>internal</b>	Displays LACP internal information.
<b>neighbor</b>	Displays information about the LACP neighbor.
<b>detail</b>	(Optional) Displays detailed internal information when used with the <b>internal</b> keyword and detailed LACP neighbor information when used with the <b>neighbor</b> keyword.
<b>multi-chassis</b>	Displays information about mLACP.
<b>load-balance</b>	Displays mLACP load balance information.
<b>group</b>	Displays mLACP redundancy group information,

<i>number</i>	Integer value used with the <b>group</b> and <b>port-channel</b> keywords. <ul style="list-style-type: none"> <li>• Values from 1 to 4294967295 identify the redundancy group.</li> <li>• Values from 1 to 564 identify the port-channel interface.</li> </ul>
<b>port-channel</b>	Displays mLACP port-channel information.
<b>sys-id</b>	Displays the LACP system identification. It is a combination of the port priority and the MAC address of the device

**Command Modes**

User EXEC (&gt;) Privileged EXEC (#)

**Command History**

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 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.
12.2(33)SRE	This command was modified. The <b>multi-chassis</b> , <b>group</b> , and <b>port-channel</b> keywords and <i>number</i> argument were added.
15.1(3)S	This command was modified. The <b>load-balance</b> keyword was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines**

Use the **show lacp** command to troubleshoot problems related to LACP in a network.

If you do not specify a value for the argument *channel-group-number*, all channel groups are displayed. Values in the range of 257 to 282 are supported on the CSM and the FWSM only.

## Examples

### Examples

This example shows how to display the LACP system identification using the **show lacp sys-id** command:

```
Device> show lacp sys-id
```

```
8000,AC-12-34-56-78-90
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address that is associated to the system.

## Examples

This example shows how to display the LACP statistics for a specific channel group:

```
Device# show lacp 1 counters
```

Port	LACPDUs		Marker		LACPDUs	
	Sent	Recv	Sent	Recv	Pkts	Err
Channel group: 1						
Fa4/1	8	15	0	0	3	0
Fa4/2	14	18	0	0	3	0
Fa4/3	14	18	0	0	0	
Fa4/4	13	18	0	0	0	

The output displays the following information:

- The LACPDUs Sent and Recv columns display the LACPDUs that are sent and received on each specific interface.
- The LACPDUs Pkts and Err columns display the marker-protocol packets.

The following example shows output from a **show lacp channel-group-number counters** command:

```
Device1# show lacp 5 counters
```

Port	LACPDUs		Marker		Marker Response		LACPDUs	
	Sent	Recv	Sent	Recv	Sent	Recv	Pkts	Err
Channel group: 5								
Gi5/0/0	21	18	0	0	0	0	0	

The following table describes the significant fields shown in the display.

**Table 44: show lacp channel-group-number counters Field Descriptions**

Field	Description
LACPDUs Sent Recv	Number of LACP PDUs sent and received.
Marker Sent Recv	Attempts to avoid data loss when a member link is removed from an LACP bundle.
Marker Response Sent Recv	Cisco IOS response to the Marker protocol.
LACPDUs Pkts Err	Number of LACP PDU packets transmitted and the number of packet errors.

The following example shows output from a **show lacp internal** command:

```
Device1# show lacp 5 internal
```

```
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode           P - Device is in Passive mode
```

```
Channel group 5
```

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port State
Gi5/0/0	SA	bndl	32768	0x5	0x5	0x42	0x3D

The following table describes the significant fields shown in the display.

**Table 45: show lacp internal Field Descriptions**

Field	Description
Flags	Meanings of each flag value, which indicates a device activity.
Port	Port on which link bundling is configured.
Flags	Indicators of device activity.
State	Activity state of the port. States can be any of the following: <ul style="list-style-type: none"> <li>• Bndl--Port is attached to an aggregator and bundled with other ports.</li> <li>• Susp--Port is in suspended state, so it is not attached to any aggregator.</li> <li>• Indep--Port is in independent state (not bundled but able to switch data traffic). This condition differs from the previous state because in this case LACP is not running on the partner port.</li> <li>• Hot-sby--Port is in hot standby state.</li> <li>• Down--Port is down.</li> </ul>
LACP port Priority	Priority assigned to the port.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port Number	Number of the port.

Field	Description
Port State	<p>State variables for the port that are encoded as individual bits within a single octet with the following meaning:</p> <ul style="list-style-type: none"> <li>• bit0: LACP_Activity</li> <li>• bit1: LACP_Timeout</li> <li>• bit2: Aggregation</li> <li>• bit3: Synchronization</li> <li>• bit4: Collecting</li> <li>• bit5: Distributing</li> <li>• bit6: Defaulted</li> <li>• bit7: Expired</li> </ul>

## Examples

This example shows how to display internal information for the interfaces that belong to a specific channel:

Device# **show lacp 1 internal**

Flags: S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.  
 A - Device is in Active mode. P - Device is in Passive mode.

Channel group 1

Port	Flags	State	LACPDUs Interval	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State
Fa4/1	saC	bndl	30s	32768	100	100	0xc1	0x75
Fa4/2	saC	bndl	30s	32768	100	100	0xc2	0x75
Fa4/3	saC	bndl	30s	32768	100	100	0xc3	0x75
Fa4/4	saC	bndl	30s	32768	100	100	0xc4	0x75

Device#

The following table describes the significant fields shown in the display.

**Table 46: show lacp internal Field Descriptions**

Field	Description
State	<p>Current state of the port; allowed values are as follows:</p> <ul style="list-style-type: none"> <li>• bndl--Port is attached to an aggregator and bundled with other ports.</li> <li>• susp--Port is in a suspended state; it is not attached to any aggregator.</li> <li>• indep--Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).</li> <li>• hot-sby--Port is in a hot-standby state.</li> <li>• down--Port is down.</li> </ul>
LACPDUs Interval	Interval setting.
LACP Port Priority	Port-priority setting.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port Number	Port number.
Port State	<p>Activity state of the port.</p> <ul style="list-style-type: none"> <li>• See the Port State description in the show lacp internal Field Descriptions table for state variables.</li> </ul>

**Examples**

This example shows how to display the information about the LACP neighbors for a specific port channel:

```
Device# show lacp 1 neighbors
```

```
Flags: S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
       A - Device is in Active mode.       P - Device is in Passive mode.
```

```
Channel group 1 neighbors
```

Port	Partner System ID	Partner Port Number	Age	Flags
Fa4/1	8000,00b0.c23e.d84e	0x81	29s	P
Fa4/2	8000,00b0.c23e.d84e	0x82	0s	P
Fa4/3	8000,00b0.c23e.d84e	0x83	0s	P
Fa4/4	8000,00b0.c23e.d84e	0x84	0s	P

  

Port	Admin Key	Oper Key	Port State
Fa4/1	32768	200	0x81

```

Fa4/2      32768      200      200      0x81
Fa4/3      32768      200      200      0x81
Fa4/4      32768      200      200      0x81
Device#

```

The following table describes the significant fields shown in the display.

**Table 47: show lacp neighbors Field Descriptions**

Field	Description
Port	Port on which link bundling is configured.
Partner System ID	Peer's LACP system identification (sys-id). It is a combination of the system priority and the MAC address of the peer device.
Partner Port Number	Port number on the peer device
Age	Number of seconds since the last LACP PDU was received on the port.
Flags	Indicators of device activity.
Port Priority	Port priority setting.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port State	Activity state of the port.  See the Port State description in the show lacp internal Field Descriptions table for state variables.

If no PDUs have been received, the default administrative information is displayed in braces.

#### Related Commands

Command	Description
<b>clear lacp counters</b>	Clears the statistics for all interfaces belonging to a specific channel group.
<b>lacp port-priority</b>	Sets the priority for the physical interfaces.
<b>lacp system-priority</b>	Sets the priority of the system.



# show lldp

To display information about one or all neighboring devices discovered using Link Layer Discovery Protocol (LLDP), use the **show lldp** command in privileged EXEC mode.

**show lldp** [**entry** {**\***| *word*}| **errors**| **interface** [**ethernet** *number*]| **neighbors** [**ethernet** *number*| **detail**]| **traffic**]

## Syntax Description

<b>entry</b>	(Optional) Displays detailed information for a specific neighbor entry.
<b>*</b>	(Optional) Displays detailed information about all the LLDP neighbors.
<i>word</i>	(Optional) Name of the neighbor about which information is requested.
<b>errors</b>	(Optional) Displays LLDP computational errors and overflows.
<b>interface</b>	(Optional) Displays status and configuration of an interface on which LLDP is enabled.
<b>ethernet</b>	(Optional) Displays an IEEE 802.3 interface on which LLDP is enabled.
<i>number</i>	(Optional) Integer that identifies the interface.
<b>neighbors</b>	(Optional) Displays neighbor entries.  <b>Note</b> If the device ID has more than 20 characters, the ID will be truncated to 20 characters in command output because of display constraints.
<b>detail</b>	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled capabilities, hold time, and software version.
<b>traffic</b>	(Optional) Displays LLDP statistics.

## Command Modes

Privileged EXEC (#)

**Command History**

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(50)SY	Modified <b>show lldp neighbors detail</b> output to parse and display management addresses OID in ASN.1 notation.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

**Usage Guidelines**

Use this command to monitor LLDP activity in a network.

When you use the **neighbors** keyword, the device ID is truncated to 20 characters in the command output because of display constraints. The **show lldp neighbors** command functions correctly; only the device ID display is truncated. For detailed neighbor information, use the **show lldp neighbors detail** command.

**Examples**

The following is sample output from the **show lldp entry \*** command. Information about all the LLDP neighbors is displayed, including device ID, capabilities, addresses, hold time, and version.

```
Device# show lldp entry *
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Chassis id: aabb.cc00.1f01
Port id: Et1/0
Port Description: Ethernet1/0
System Name: R1.example.com
System Description:
Cisco IOS Software, Solaris Software (UNIX-JS-M)
12.2(20070524:210936) [user1-sierra-0522 105]
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 25-May-07 10:52 by user1
Time remaining: 136 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses - not advertised
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
-----
Total entries displayed: 1
The table below describes the significant fields in the output.
```

**Table 48: show lldp entry \* Field Descriptions**

Field	Description
Capability Codes	Type of device that can be discovered. Possible values are as follows: R--Router B--Bridge T--Telephone C--DOCSIS Cable Device W--WLAN Access Point P--Repeater S--Station O--Other
Chassis id	Identifier assigned to the device.
Port id	Identifier of the interface.
Port Description	Description of the interface.
System Name	Name of the device within the network.
System Description	Description of the software operating on the device.
Time remaining	Time remaining before the information is aged out.
System Capabilities	Possible capabilities of the device.
Enabled Capabilities	Subset of possible capabilities that are enabled.
Management Addresses	Layer 3 addresses of the management interface.
Auto Negotiation	Supported and enabled status of all interface autonegotiation capabilities.
Physical media capabilities	Physical characteristics of the interface on which LLDP operates.
Media Attachment Unit type	Numeric value representing the type of the media attachment unit.
Total entries displayed	Number of neighbor devices for which information is displayed.

The following is sample output from the **show lldp neighbors** command showing information about neighboring devices discovered using LLDP.

```
Device# show lldp neighbors

Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf    Hold-time    Capability    Port ID
R1             Et1/0        150          R             Et1/0

Total entries displayed: 1
```

The table below describes the significant fields shown in the output.

**Table 49: show lldp neighbors Field Descriptions**

Field	Description
Capability Codes	See the show lldp entry * Field Descriptions table for details.
Device ID	Name of the neighbor device. <b>Note</b> If the device ID has more than 20 characters, the ID will be truncated to 20 characters in command output because of display constraints.
Local Intf	Local interface through which this neighbor is connected.
Hold-time	Amount of time (in seconds) the current device will hold the LLDP advertisement from a sending device before discarding it.
Capability	Type of device listed in the LLDP Neighbors table. Values correspond to the values of the capability codes.
Port ID	Interface and port number of the neighboring device.
Total entries displayed	Number of neighbor devices for which information is displayed.

The following is sample output from the **show lldp neighbors detail** command showing information about neighboring devices discovered using LLDP:

```
Device# show lldp neighbors detail

-----
Chassis id: aabb.cc00.6502
Port id: Et2/0
Port Description: Ethernet2/0
System Name: r101

System Description:
```

```

Cisco IOS Software, Solaris Software (UNIX-P-M), Experimental Version 12.2(20081021:182811)
[yonhan-CSCsm33589-flo_dsgs7 105]
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 31-Oct-08 11:20 by yonhan

```

```

Time remaining: 105 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses:
  IP: 192.168.1.1
  OID:
    1.3.6.1.4.1.16361.1.69.2.2.

```

Auto

The table below describes the significant fields shown in the output.

**Table 50: show lldp neighbors detail Field Descriptions**

Field	Description
Chassis id	Identifier assigned to the device.
Port id	Identifier of the interface.
Port Description	Description of the interface.
System Name	Name of the device within the network.
System Description	Description of the software operating on the device.
Time remaining	Time remaining before the information is aged out.
System Capabilities	Possible capabilities of the device.
Enabled Capabilities	Subset of possible capabilities that are enabled.
Management Addresses	Layer 3 addresses of the management interface.
Auto	Supported and enabled status of all interface autonegotiation capabilities.

The following is sample output from the **show lldp interface** command for Ethernet interface 0/1:

```

Device# show lldp interface ethernet 0/1

Ethernet0/1:
  Tx: enabled
  Rx: enabled
  Tx state: IDLE
  Rx state: WAIT FOR FRAME

```

The table below describes the significant fields shown in the output.

**Table 51: show lldp interface Field Descriptions**

Field	Description
Tx	Ability of the interface to transmit advertisements.

Field	Description
Rx	Ability of the interface to receive advertisements.
Tx state	Current finite state machine state of the interface in transmit mode.
Rx state	Current finite state machine state of the interface in receive mode.

The following is sample output from the **show lldp errors** command:

```
Device# show lldp errors
LLDP errors/overflows:
  Total memory allocation failures: 0
  Total encapsulation failures: 0
  Total input queue overflows: 0
  Total table overflows: 0
```

The table below describes the significant fields shown in the output.

**Table 52: show lldp errors Field Descriptions**

Field	Description
Total memory allocation failures	Number of memory allocation failures.
Total encapsulation failures	Number of LLDP packet encapsulation failures.
Total input queue overflows	Number of times incoming advertisements exceeded the capacity of the LLDP input queue.
Total table overflows	Number of times the LLDP table rejected advertisements because it was full.

The following is sample output from the **show lldp traffic** command:

```
Device# show lldp traffic
LLDP traffic statistics:
  Total frames out: 277
  Total entries aged: 0
  Total frames in: 328
  Total frames received in error: 0
  Total frames discarded: 0
  Total TLVs unrecognized: 0
```

The table below describes the significant fields shown in the output.

**Table 53: show lldp traffic Field Descriptions**

Field	Definition
Total frames out	Number of advertisements sent from the device.

Field	Definition
Total entries aged	Number of neighbor device entries aged out.
Total frames in	Number of advertisements received by the device.
Total frames received in error	Number of times the LLDP advertisements contained errors of any type.
Total frames discarded	Number of times the LLDP process discarded an incoming advertisement.
Total TLVs unrecognized	Number of TLVs that could not be processed because the content of the TLV was not recognized by the device or the content fields were incorrectly specified.

# show nmosp

To display the Network Mobility Services Protocol (NMSP) information, use the **shownmosp** command in privileged EXEC mode.

**show nmosp** {**attachment suppress interface**| **capability**| **notification interval**| **statistics** {**connection**| **summary**}}| **status**| **subscription** {**detail**| **summary**}}

## Syntax Description

<b>attachment suppress interface</b>	Displays attachment suppress interfaces.
<b>capability</b>	Displays switch capabilities including the supported services and subservices.
<b>notification interval</b>	Displays the notification intervals of the supported services.
<b>statistics</b>	Displays the NMSP statistics information. <ul style="list-style-type: none"> <li>• <b>connection</b> --Displays the message counters on each connection.</li> <li>• <b>summary</b> --Displays the global counters.</li> </ul>
<b>status</b>	Displays information about the NMSP connections.
<b>subscription</b>	Displays the subscription information on each NMSP connection. <ul style="list-style-type: none"> <li>• <b>detail</b> --Displays all services and subservices subscribed on each connection.</li> <li>• <b>summary</b> --Displays all services subscribed on each connection.</li> </ul>

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(55)SE	This command was modified. The output was enhanced to display all the interfaces that have been suppressed after the CDP Server TLV exchange takes place.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.



## Usage Guidelines

You can use the Cisco IOS software output modifiers to filter the output of the **shownmsp** command, to display only those lines you are interested in.

The output modifier feature is invoked by using the pipe symbol (`|`). To use this feature, enter the **shownmsp** command with a space and the pipe symbol at the end of the command line, followed by one of the keywords shown in the table below.

**Table 54: Using Output Modifiers**

Command	Purpose
<b>append</b> <i>regular-expression</i>	Appends redirected output to URL (only to the URLs supporting the append operation).
<b>begin</b> <i>regular-expression</i>	Displays the first line that matches the regular expression, and then all other lines that follow that line.
<b>include</b> <i>regular-expression</i>	Displays all lines that match the regular expression.
<b>exclude</b> <i>regular-expression</i>	Displays all lines except those that match the regular expression.
<b>format</b> <i>regular-expression</i>	Formats the output using the specification file.
<b>redirect</b> <i>regular-expression</i>	Redirects the output to the URL.
<b>section</b> <i>regular-expression</i>	Filters a section of the output.
<b>tee</b> <i>regular-expression</i>	Copies output to the URL.

## Examples

The following is sample output from the **shownmspattachmentsuppressinterface** command:

```
Device# show nmsp attachment suppress interface
NMSP Attachment Suppression Interfaces
-----
GigabitEthernet1/0/10    CLI Suppressed
GigabitEthernet1/0/11    Internal Suppressed
```

The following is sample output from the **shownmspcapability** command:

```
Device# show nmsp capability
NMSP Switch Capability
-----
Service      Subservice
-----
Attachment   Wired Station
Location     Subscription
```

The following is sample output from the **shownmspnotificationinterval** command:

```
Device# show nmsp notification interval
```

## NMSP Notification Intervals

```
-----
Attachment notify interval: 30 sec (default)
Location notify interval: 30 sec (default)
```

The following is sample output from the

**shownmospstatisticsconnectionandshownmospstatisticssummary** commands:

```
Device# show nmosp statistics connection
```

```
NMSP Connection Counters
```

```
-----
Connection 1:
```

```
Connection status: UP
Freed connection: 0
Tx message count      Rx message count
```

```
-----
Subscr Resp: 1          Subscr Req: 1
Capa Notif: 1           Capa Notif: 1
Atta Resp: 1            Atta Req: 1
Atta Notif: 0
Loc Resp: 1             Loc Req: 1
Loc Notif: 0
```

```
Unsupported msg: 0
```

```
Device# show nmosp statistics summary
```

```
NMSP Global Counters
```

```
-----
Send too big msg: 0
Failed socket write: 0
Partial socket write: 0
Socket write would block: 0
Failed socket read: 0
Socket read would block: 0
Transmit Q full: 0
Max Location Notify Msg: 0
Max Attachment Notify Msg: 0
```

```
Max Tx Q Size: 0
```

The following is sample output from the **shownmospstatus** command:

```
Device# show nmosp status
```

```
NMSP Status
```

```
-----
NMSP: enabled
```

```
MSE IP Address      TxEchoResp RxEchoReq TxData RxData
172.19.35.109      5 5 4 4
```

The following is sample output from the

**shownmospshowsubscriptiondetailandtheshownmospshowsubscriptionsummary** commands:

```
Device# show nmosp subscription detail
```

```
Mobility Services Subscribed by 172.19.35.109:
```

```
Services              Subservices
```

```
-----
Attachment:           Wired Station
Location:              Subscription
```

```
Device# show nmosp subscription summary
```

```
Mobility Services Subscribed:
```

```
MSE IP Address      Services
```

```
-----
172.19.35.109      Attachment, Location
```

## Related Commands

Command	Description
<b>clear nmosp statistics</b>	Clears the NMSP statistic counters.
<b>nmosp</b>	Enables NMSP on a switch.



# show ptp clock dataset

To display a summary of the Precision Time Protocol clock status, use the `show ptp clock dataset` command in privileged EXEC mode.

**show ptp clock dataset** [**default**| **current**]

## Cisco ASR 901 Series Aggregation Services Router

**show ptp clock dataset** {**default**| **current**}

### Syntax Description

<b>default</b>	(Optional) Displays the default PTP clock dataset. <b>Note</b> <b>default</b> On the ASR 901 Series Aggregation Services Router, you must choose either the <b>default</b> keyword or the <b>current</b> keyword.
<b>current</b>	(Optional) Displays the current PTP clock dataset. <b>Note</b> On the ASR 901 Series Aggregation Services Router, you must choose either the <b>current</b> keyword or the <b>default</b> keyword.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

Use this command to verify a PTP clocking configuration.

On the Cisco ASR 901 Series Aggregation Services Router, one of the keywords (**default** or **current**) must be used with the command.

### Examples

The following examples show the output generated by this command:

```
Device# show ptp clock dataset default

CLOCK [Boundary Clock, domain 10]
Two Step Flag: No
Clock Identity: 0x2A:0:0:0:58:67:F3:4
```

```

Number Of Ports: 1
Priority1: 89
Priority2: 90
Domain Number: 10
Slave Only: No
Clock Quality:
  Class: 224
  Accuracy: Unknown
  Offset (log variance): 4252

```

Device# **show ptp clock dataset current**

```

CLOCK [Boundary Clock, domain 10]
  Steps Removed: 18522
  Offset From Master: 4661806827187470336
  Mean Path Delay: 314023819427708928

```

The table below describes significant fields shown in the display.

**Table 55: show ptp clock dataset Field Descriptions**

Field	Description
Two Step Flag	Indicates whether the clock is sending timestamp information using a FOLLOW_UP message (a 2-step handshake) or not (a 1-step handshake).
Clock Identity	Unique identifier for the clock.
Number of Ports	Number of ports assigned to the PTP clock.
Priority1	Priority1 preference value of the PTP clock; the priority1 clock is considered first during clock selection.
Priority2	Priority2 preference value of the PTP clock; the priority2 clock is considered after all other clock sources during clock selection.
Domain number	PTP clocking domain number.
Slave only	Specifies whether the PTP clock is a slave-only clock.
Clock quality	Summarizes the quality of the grandmaster clock.
Class	Displays the time and frequency traceability of the grandmaster clock
Accuracy	Field applies only when the Best Master Clock algorithm is in use; indicates the expected accuracy of the master clock were the grandmaster clock.
Offset (log variance)	Offset between the local clock and an ideal reference clock.
Steps removed	Number of hops from the local clock to the grandmaster clock.

Field	Description
Offset From Master	Time offset between the slave and master clocks.
Mean Path Delay	Mean propagation time between the master and slave clocks.

# show ptp clock dataset parent

To display a description of the Precision Time Protocol parent clock, use the show ptp dataset parent command in privileged EXEC mode.

**show ptp clock dataset parent**

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

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	15.0(1)S	This command was introduced.
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** Use this command to verify a PTP clocking configuration.

**Examples** The following example shows the output generated by this command:

```
Device# show ptp clock dataset parent
CLOCK [Boundary Clock, domain 10]
  Parent Stats: No
  Observed Parent Offset (log variance): 0
  Observed Parent Clock Phase Change Rate: 58087144
  Grandmaster Clock:
    Identity: 0x3E:D3:D0:0:0:0:0:0
    Priority1: 42
    Priority2: 0
    Clock Quality:
      Class: 176
      Accuracy: Unknown
      Offset (log variance): 4252
```

The table below describes significant fields shown in the display.

**Table 56: show ptp clock dataset parent Field Descriptions**

Field	Description
Parent Stats	Indicates the availability of parent statistics.
Observed Parent Offset (log variance)	The offset between the parent clock and the local clock.

Field	Description
Observed Parent Clock Phase Change Rate	This value indicates the parent clock speed relative to the slave clock. A positive value indicates that the parent clock is faster than the slaveclock ; a negative value indicates that the parent clock is slower than the slave clock.
Grandmaster clock	Summarizes the Grandmaster clock configuration.
Identity	The hardware address of the Grandmaster clock.
Priority1	The priority1 preference value of the PTP clock; the priority1 clock is considered first during clock selection.
Priority2	The priority2 preference value of the PTP clock; the priority2 clock is considered after all other clock sources during clock selection.
Clock Quality	Summarizes the quality of the Grandmaster clock.
Class	Displays the time and frequency traceability of the grandmaster clock
Accuracy	This field applies only when the Best Master Clock algorithm is in use; indicates the expected accuracy of the master clock were the grandmaster clock.
Offset (log variance)	The offset between the Grandmaster clock and the parent clock.



# show ptp clock dataset time-properties

To display a summary of time properties for a Precision Time Protocol clock, use the `show ptp dataset time-properties` command in privileged EXEC mode.

**show ptp clock dataset time-properties**

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

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	15.0(1)S	This command was introduced.
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** Use this command to verify a PTP clocking configuration.

**Examples** The following example shows the output generated by this command:

```
Device# show ptp clock dataset time-properties
```

```
CLOCK [Boundary Clock, domain 10]
  Current UTC Offset Valid: TRUE
  Current UTC Offset: 10752
  Leap 59: FALSE
  Leap 61: TRUE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: Unknown
```

The table below describes significant fields shown in the display.

**Table 57: show ptp clock dataset time-properties Field Descriptions**

Field	Description
Current UTC Offset Valid	Indicates whether the current UTC offset is valid.
Current UTC Offset	Offset between the TAI and UTC in seconds.
Leap 59	Indicates whether the last minute of the current UTC day contains 59 seconds.

Field	Description
Leap 61	Indicates whether the last minute of the current UTC day contains 61 seconds.
Time Traceable	Indicates whether the value of the current UTC offset is traceable to a primary reference.
Frequency Traceable	Indicates whether the frequency used to determine the time scale is traceable to a primary reference.
PTP Timescale	Indicates whether the PTP grandmaster clock uses a PTP clock time scale.
Time Source	Time source used by the grandmaster clock.

# show ptp clock running

To display a summary of the Precision Time Protocol clock status, use the `show ptp clock running` command in privileged EXEC mode.

**show ptp clock running [domain]**

## Syntax Description

<b>domain</b>	Filters output by domain.
---------------	---------------------------

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

Use this command to verify a PTP clocking configuration.

## Examples

The following example shows the output generated by this command:

```
Device# show ptp clock running

PTP Boundary Clock [Domain 1]
      State      Ports      Pkts sent      Pkts rcvd
      FREERUN      3          1090          1023

      PORT SUMMARY
Name      Tx Mode      Role      Transport      State      Sessions
MASTER-1  unicast      master    Et0/0          -          5
MASTER-2  mcast        master    Et0/0          -          5
SLAVE      unicast      slave     Et0/0          -          5

      PTP Ordinary Clock [Domain 2]
      State      Ports      Pkts sent      Pkts rcvd
      HOLDOVER      1          2090          2023

      PORT SUMMARY
Name      Tx Mode      Role      Transport      State      Sessions
MASTER      unicast      master    Et0/0          -          5
```

The table below describes significant fields shown in the display.

**Table 58: show ptp clock running Field Descriptions**

Field	Description
State	State of the PTP clock.

Field	Description
Ports	Number of ports assigned to the PTP clock.
Pkts sent	Number of packets sent by the PTP clock.
Pkts rcvd	Number of packets received by the PTP clock.
Name	Name of the PTP clock port.
Tx Mode	Transmission mode of the PTP clock port (unicast or multicast).
Role	PTP role of the clock port (master or slave).
Transport	Physical port assigned to the clock port.
State	State of the clock port.
Sessions	Number of PTP sessions active on the clock port.

# show ptp port dataset foreign-master

To display a summary of Precision Time Protocol foreign master records, use the **show ptp port dataset foreign-master-record** command in privileged EXEC mode.

**show ptp port dataset foreign-master [domain]**

## Syntax Description

This command has no arguments or keywords.

<b>domain</b>	Filters output by domain.
---------------	---------------------------

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.0(1)S	This command was introduced.

## Usage Guidelines

Use this command to verify a PTP clocking configuration.

## Examples

The following example shows the output generated by this command.

```
Device# show ptp dataset foreign-master

PTP FOREIGN MASTER RECORDS
Interface Vlan2
Number of foreign records 1, max foreign records 5
Best foreign record 0
RECORD #0
Foreign master port identity: clock id: 0x0:1E:4A:FF:FF:96:A2:A9
Foreign master port identity: port num: 1
Number of Announce messages: 8
Number of Current Announce messages: 6
Time stamps: 1233935406, 664274927
```

The table below describes significant fields shown in the display.

**Table 59: show ptp port dataset foreign-master Field Descriptions**

Field	Description
Interface	Currently foreign-master data is not displayed in the show command.
Number of foreign records	Number of foreign master records in device memory.
max foreign records	Maximum number of foreign records.

Field	Description
Best foreign record	Foreign record with the highest clock quality.
Foreign master port identity: clock id	Hardware address of the foreign master port.
Foreign master port identity: port number	Port number of the foreign master port.
Number of Announce messages	Number of Announce messages received from the foreign master clock.
Number of Current Announce messages	Number of current announcement messages.
Time stamps	Time stamps of current announcement messages.

## show ptp port dataset port

To display a summary of Precision Time Protocol ports, use the **show ptp port dataset port** command in privileged EXEC mode.

**show ptp dataset port**

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

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	15.0(1)S	This command was introduced.

**Usage Guidelines** Use this command to verify a PTP clocking configuration.

**Examples** The following example shows the output generated by this command.

```
Device# show ptp port dataset port

PORT [MASTER]
  Clock Identity: 0x49:BD:D1:0:0:0:0:0
  Port Number: 0
  Port State: Unknown
  Min Delay Req Interval (log base 2): 42
  Peer Mean Path Delay: 648518346341351424
  Announce interval (log base 2): 0
  Announce Receipt Timeout: 2
  Sync Interval (log base 2): 0
  Delay Mechanism: End to End
  Peer Delay Request Interval (log base 2): 0
  PTP version: 2
```

The table below describes significant fields shown in the display.

**Table 60: show ptp port dataset port Field Descriptions**

Field	Description
Clock Identity	Unique identifier for the clock.
Port Number	Port number on the PTP node.
Port State	State of the PTP port.
Min Delay Req Interval (log base 2)	Time interval permitted between Delay_Req messages.

Field	Description
Peer Mean Path Delay	One way propagation delay on the local port.
Announce interval (log base 2)	Mean interval between PTP announcement messages.
Announce Receipt Timeout	Number of intervals before a PTP announcement times out.
Sync Interval (log base 2)	Mean interval between PTP sync messages.
Delay Mechanism	Mechanism used for measuring propagation delay.
Peer Delay Request Interval (log base 2)	Interval permitted between Peer Delay Request messages.
PTP version	PTP version in use.



## shutdown (bridge-domain)

To change the administrative state of a bridge domain from in service to out of service, use the **shutdown** command in bridge-domain configuration mode. To change the administrative state of a bridge domain from out of service to in service, use the **no** form of this command.

**shutdown**

**no shutdown**

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

**Command Default** The bridge domain is in service.

**Command Modes** Bridge-domain configuration (config-bdomain)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

**Usage Guidelines** Use the **shutdown** command to disable the Layer 2 multipoint bridging service associated with a bridge domain. When a bridge domain is shut down, the state of all service instances bound to it and the bridge domain's corresponding bridge domain interface (BDI) are also shut down.

**Examples** The following example shows how to change the administrative state of bridge domain 5 from in service to out of service:

```
Router(config)# bridge-domain 5
Router(config-bdomain)# shutdown
```

# snmp-server enable traps ethernet cfm alarm

To enable Ethernet connectivity fault management (CFM) fault alarms (traps), use the **snmp-server enable traps ethernet cfm alarm** command in global configuration mode. To disable fault alarms, use the **no** form of this command.

**snmp-server enable traps ethernet cfm alarm**

**no snmp-server enable traps ethernet cfm alarm**

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

**Command Default** Alarms are disabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(33)SRD	This command was introduced.
	12.2(54)SE	This command was integrated into Cisco IOS Release 12.2(54)SE.
	15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
	Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

**Usage Guidelines** Use this command to turn on or turn off CFM fault alarms.

**Examples** The following example shows how to enable CFM fault alarms:

```
Device(config)#  
snmp-server enable traps ethernet cfm alarm
```

## snmp-server enable traps ethernet cfm cc

To enable Simple Network Management Protocol (SNMP) trap generation for Ethernet connectivity fault management (CFM) continuity check events, use the **snmp-server enable traps ethernet cfm cc** command in global configuration mode. To disable SNMP trap generation for Ethernet CFM continuity check events, use the **no** form of this command.

**snmp-server enable traps ethernet cfm cc** [**config**] [**cross-connect**] [**loop**] [**mep-down**] [**mep-up**]

**no snmp-server enable traps ethernet cfm cc** [**config**] [**cross-connect**] [**loop**] [**mep-down**] [**mep-up**]

### Syntax Description

<b>config</b>	(Optional) Generates a trap when a CFM misconfiguration exists in the network.
<b>cross-connect</b>	(Optional) Generates a trap when a cross-connected service exists in the network.
<b>loop</b>	(Optional) Generates a trap when a forwarding loop exists in the network.
<b>mep-down</b>	(Optional) Generates a trap when a device has lost connectivity with a remote MEP or when connectivity from a previously learned remote MEP is restored after interruption.
<b>mep-up</b>	(Optional) Generates a trap when a new remote maintenance endpoint (MEP) has been discovered and learned by the device or when a change occurs in the port state of a previously discovered remote MEP.

### Command Default

When no options are configured, all continuity check traps are enabled.

### 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)SX12	This command was integrated into Cisco IOS Release 12.2(33)SX12.

Release	Modification
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

The configuration error trap (cEtherCfmCcConfigError) is triggered when a device receives a CCM that has the same MPID as a locally configured MEP but a different source MAC Address than its own. The configuration error trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of local MEP that has the same ID as that received in the CCM.
- Name of the interface on which the MEP above is configured.
- MAC Address of the remote device sending the CCM.

The cross-connect service trap (cEtherCfmCcCrossconnect) is generated when a device receives a continuity check message (CCM) whose service ID is different from what is locally configured on the device for the given service VLAN (S-VLAN). This mismatch indicates that there could be a cross-connected service in the network. The trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of remote MEP causing the alarm to be raised.
- MAC address of remote MEP causing the alarm to be raised.
- Service ID reported by the remote MEP.

The loop trap (cEtherCfmCcLoop) is generated when a device receives a CCM that has the same source MAC Address and MPID as its own, thereby indicating that the device is receiving its own CCMs and that a forwarding loop exists in the network. The loop trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of the MEP originating the CCM.
- Name of the interface on which the MEP above is configured.

The mep-down trap (cEtherCfmCcMepDown) notifies the NMS that the device has lost connectivity with a remote MEP. This trap also serves as a clear for Loop, Config, Cross-Connect and Unknown-MEP events.

The mep-down trap is generated in the following cases:

- A valid CCM with a zero hold-time is received from a remote MEP, and the device either has a valid (non-expired) CCDB entry for that MEP or does not have any CCDB entry. In other words, the trap is not generated for an already expired CCDB entry. This trigger has the event code "lastGasp."
- An entry for a remote MEP in the CCDB expires and is archived. This trigger has the event code "timeout."
- A previous configuration error trap is cleared. This trigger has the event code "configClear."
- A previous loop trap is cleared. This trigger has the event code "loopClear."
- A previous Crossconnect trap is cleared. This trigger has the event code "xconnectClear."
- A previous unknown trap is cleared. This trigger has the event code "unknownClear."

The mep-down trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- A count of the local MEPs on the same domain and S-VLAN as the remote MEP that are affected by the event.
- A count of the different interfaces on which the local MEPs above are configured.
- MPID of the remote MEP that is being reported down.
- MAC address of the remote MEP that is being reported down.
- Event code indicating one of the following: lastGasp, timeout, configClear, loopClear, xconnectClear, unknownClear.

The mep-up trap (cEtherCfmCcMepUp) serves three functions. One function is to notify the network management system (NMS) that a new MEP has been discovered and learned by the device. The second function is that the trap notifies the NMS that there is a change in the port-state of a previously discovered remote MEP. The third is to notify the NMS when connectivity from a previously discovered MEP is restored after interruption.

Mep-up traps are suppressed while cross-check is operational because the cross-check traps more efficiently convey the status of the service.

The mep-up trap is generated in the following cases:

- A valid CCM with a non-zero hold-time is received from a remote MEP for the first time, and hence an entry is created for that MEP in the continuity check database (CCDB). This trigger has the event code "new."
- A valid CCM with a non-zero hold-time is received from a remote MEP for which the device has an expired entry in the CCDB (that is, the device has an entry for that remote MEP in the archived DB). This trigger has the event code "returning."
- A valid CCM with a non-zero hold-time is received from a remote MEP for which the device has a valid entry in the CCDB and the port-state indicated in the CCM is different from what is cached in the CCDB. This trigger has the event code "portState"

The mep-up trap includes the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- The MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- A count of the local MEPs on the same domain and S-VLAN as the remote MEP that are affected by the event.
- A count of the different interfaces on which the local MEPs above are configured.
- MPID of the remote MEP that is being reported up.
- MAC address of the remote MEP that is being reported up.
- Event code indicating one of the following: new MEP, returning MEP, or port-state change.
- Port state of remote MEP.

### Examples

The following example shows how to enable SNMP trap generation for Ethernet CFM continuity checks when a new remote MEP is discovered and learned by the device:

```
Device(config)# snmp-server enable traps ethernet cfm cc mep-up
```

## snmp-server enable traps ethernet cfm crosscheck

To enable Simple Network Management Protocol (SNMP) trap generation for Ethernet connectivity fault management (CFM) continuity check events, in relation to the cross-check operation between statically configured maintenance endpoints (MEPs) and those learned via continuity check messages (CCMs), use the **snmp-server enable traps ethernet cfm crosscheck** command in global configuration mode. To disable SNMP trap generation for these continuity check events, use the **no** form of this command.

**snmp-server enable traps ethernet cfm crosscheck [mep-missing] [mep-unknown] [service-up]**

**no snmp-server enable traps ethernet cfm crosscheck [mep-missing] [mep-unknown] [service-up]**

### Syntax Description

<b>mep-missing</b>	(Optional) Generates a trap when the cross-check enable timer expires and no CCMs were received from an expected (configured) MEP. One trap is generated per remote MEP.
<b>mep-unknown</b>	(Optional) Generates a trap when an unexpected (unconfigured) MEP comes up. One trap is generated per remote MEP.
<b>service-up</b>	(Optional) Generates a trap when all remote MEPs belonging to a service instance come up.

### Command Default

This command is disabled.

When no options are configured, all continuity check event traps are enabled.

### 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)SX12	This command was integrated into Cisco IOS Release 12.2(33)SX12.
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

For this class of traps to function, cross-check must be enabled on the device. Otherwise, none of these traps will be generated, even if they are configured.

The MEP-missing trap (cEtherCfmXCheckMissing) notifies the network management system (NMS) that the device did not receive any CCMs from a remote MEP that it was expecting to be part of the service instance.

The MEP-missing trap is generated in the following case:

- After enabling cross-check (**ethernet cfm mep crosscheck enable**), the device waits for the cross-check-start timeout value specified (**ethernet cfm mep crosscheck enable-timeout**). When the timeout period has elapsed, the device will cross-check the list of remote MEPs it has learned via CCMs against the static list that has been configured (**mep crosscheck mpid vlan**). For each remote MEP that is configured in the static list and for which the device has not received a CCM, a mep-missing trap is generated. The MEP-missing trap has the following fields:
- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of the remote MEP that is being reported missing.
- MAC address of the remote MEP that is being reported missing.

The mep-unknown trap (cEtherCfmXCheckUnknown) notifies the NMS that the device received CCMs from a remote MEP that it was not expecting to be part of the service instance.

The mep-unknown trap is generated in the following case:

- After cross-check is in an operational state, the device dynamically examines the list of statically configured remote MEPs against what it learns from CCMs. This occurs after cross-check is enabled and the timer has expired. When the device receives a CCM with non-zero hold time from a remote MEP that does not exist in the static list, the device raises a mep-unknown trap.

The mep-unknown trap has the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.
- MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.
- MPID of the remote MEP that is being reported unknown.
- MAC address of the remote MEP that is being reported unknown.

The service-up trap (cEtherCfmXCheckServiceUp) notifies the NMS that the device received CCMs from all remote MEPs within a given service instance.

The service-up trap is generated in the following case:

- When the device receives CCMs from all remote statically configured MEPs before the expiration of the crosscheck enable-timeout period.

The service-up trap has the following fields:

- Service ID designating the customer service instance to which the event belongs, as configured on the device reporting the event.



- MAC address of the device reporting the event. This is typically the Bridge Brain MAC address.

## Examples

The following example shows how to enable SNMP trap generation for Ethernet CFM continuity check events when an unexpected (unconfigured) MEP comes up:

```
Device (config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown
```

## Related Commands

Command	Description
<b>ethernet cfm mep crosscheck enable</b>	Enables cross checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs.
<b>mep crosscheck mpid vlan</b>	Statically defines a remote MEP within a maintenance domain.

## snmp-server enable traps ethernet evc

To enable Simple Network Management Protocol (SNMP) Ethernet virtual circuit (EVC) traps, use the **snmp-server enable traps ethernet evc** command in global configuration mode. To disable SNMP EVC traps, use the **no** form of this command.

**snmp-server enable traps ethernet evc** [**create**] [**delete**] [**status**]

**no snmp-server enable traps ethernet evc**

### Syntax Description

<b>create</b>	(Optional) Enables SNMP EVC create traps.
<b>delete</b>	(Optional) Enables SNMP EVC delete traps.
<b>status</b>	(Optional) Enables SNMP EVC status traps.

### Command Default

Trap notifications are not sent.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

### Usage Guidelines

Use this command to turn on or turn off SNMP EVC traps.

### Examples

The following example shows how to enable SNMP Ethernet EVC traps to be created:

```
Device# configure terminal
Device(config)#
snmp-server enable traps ethernet evc create
```

### Related Commands

<b>snmp-server host traps eve</b>	Enables EVC trap notifications to a specific SNMP host.
-----------------------------------	---

## snmp-server enable traps ether-oam

To enable Ethernet Operations, Administration, and Maintenance (OAM) MIB traps, use the **snmp-server enable traps ether-oam** command in global configuration mode. To disable OAM MIB traps, use the **no** form of this command.

**snmp-server enable traps ether-oam**

**no snmp-server enable traps ether-oam**

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

**Command Default** OAM traps are disabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	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.

**Usage Guidelines** A trap will not be sent if a trap was sent within the last 1 second.

**Examples** The following example shows how to enable OAM MIB traps:

```
Device# configure terminal
Device(config)# snmp-server enable traps ether-oam
```

## snmp-server host traps evc

To enable Ethernet virtual circuit (EVC) trap notifications to a specific Simple Network Management Protocol (SNMP) host, use the **snmp-server host traps evc** command in global configuration mode. To disable EVC trap notifications to a specific host, use the **no** form of this command.

**snmp-server host** *ipaddr* **traps** *string* **evc**

**no snmp-server host** *ipaddr* **traps** *string*

### Syntax Description

<i>ipaddr</i>	IPv4 or IPv6 address of the SNMP notification host.
<i>string</i>	SNMPv1 community string, SNMPv2c community string, or SNMPv3 username.

### Command Default

EVC trap notifications are not sent to an SNMP host.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

### Usage Guidelines

Use this command to start or stop sending EVC traps to a specific SNMP host.

### Examples

The following example shows how to enable EVC trap notifications to an SNMP host:

```
Device# configure terminal
Device(config)# snmp-server host 172.17.2.0 traps snmp-host01 evc
```

### Related Commands

<b>snmp-server enable traps ethernet evc</b>	Enables SNMP EVC traps.
--	-------------------------

## source template (eoam)

To associate a template to an Ethernet operations, maintenance, and administration (OAM) interface, use the **source template (eoam)** command in interface configuration mode. To remove the source template association, use the **no** form of this command.

**source template** *template-name*

**no source template** *template-name*

### Syntax Description

<i>template-name</i>	String that identifies the source template.
----------------------	---

### Command Default

No source template is configured.

### 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.

### Usage Guidelines

When this command is used, the interface inherits all the configurations in the template. A benefit of using a source template is that it helps reduce the overall configuration size by grouping repeating commands.

### Examples

The following example shows how to create a source template named oam on OAM interface Ethernet 0/1:

```
Device(config)# interface ethernet 0/1
Device(config-if)# source
template oam
```

### Related Commands

<b>template (eoam)</b>	Configures a template for use on Ethernet OAM interfaces and places the device in configuration template mode.
------------------------	--



# status decoupled

To enable decoupled mode so that the state of the attachment circuits (ACs) on the user-facing provider edge (UPE) device is decoupled from the state of the pseudowire connections, use the **status decoupled** command in the appropriate configuration mode. To disable decoupled mode, use the **no** form of this command.

**status decoupled**

**no status decoupled**

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

**Command Default** The default is coupled mode.

**Command Modes**

- Interface configuration (config-if)
- Pseudowire class configuration (config-pw-class)
- Template configuration (config-template)
- VFI configuration (config-vfi)

Command History	Release	Modification
	12.2(33)SRE	This command was introduced.
	Cisco IOS XE Release 3.7S	The command was modified. This command was modified as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes.
	15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

**Usage Guidelines** Coupled and decoupled modes are defined as follows:

- **Coupled Mode**—When at least one AC in the virtual forwarding interface (VFI) changes state to Active, all pseudowires in the VFI advertise Active. When all ACs in the VFI change state to standby, all pseudowires in the VFI will advertise standby mode.
- **Decoupled Mode**—All the pseudowires in the VFI are always active, and the AC state is independent of the pseudowire state. The AC state can be enabled if the peer does not support pseudowire preferential forwarding (standby) circuit status. The lack of support for pseudowire preferential forwarding (standby) circuit status provides lower switchover time at the cost of extra flooding or multicast that affects the peer provider edge (PE) with standby ACs.

The multichassis Link Aggregation Control Protocol (mLACP) controls the state of the ACs.

## Examples

The following example shows how to enable the decoupled mode in pseudowire class configuration mode:

```
Device(config)# pseudowire-class mpls-dhd
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# status peer topology dual-homed
Device(config-pw-class)# status decoupled
```

The following example shows how to enable the decoupled mode in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# status peer topology dual-homed
Device(config-if)# status decoupled
```

The following example shows how to enable the decoupled mode in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# status peer topology dual-homed
Device(config-template)# status decoupled
```

## Related Commands

Command	Description
<b>encapsulation (pseudowire)</b>	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
<b>l2 vfi manual</b>	Enters VFI configuration mode and establishes a Layer 2 virtual forwarding interface between two separate networks.
<b>pseudowire-class</b>	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.



# status peer topology dual-homed

To enable the reflection of the attachment circuit status on both the primary and secondary pseudowire connections, use the **status peer topology dual-homed** command in the appropriate configuration mode. To disable the reflection status, use the **no** form of this command.

**status peer topology dual-homed**

**no status peer topology dual-homed**

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

**Command Default** The reflection of the attachment circuit status on the primary and secondary pseudowire connections is disabled.

**Command Modes**

- Interface configuration (config-if)
- Pseudowire class configuration (config-pw-class)
- Template configuration (config-template)

Command History	Release	Modification
	12.2(33)SRE	This command was introduced.
	Cisco IOS XE Release 3.7S	This command was modified. This command was modified as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in interface pseudowire configuration and template configuration modes.
	15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

**Usage Guidelines** The **status peer topology dual-homed** command must be entered if the peer provider edge (PE) devices are connected to a dual-homed device.

**Examples**

The following example shows how to enter pseudowire class configuration mode and configure the status peer topology for dual-homed operation:

```
Device(config)# pseudowire-class mpls-dhd
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# status peer topology dual-homed
```

The following example shows how to enter interface configuration mode and configure the status peer topology for dual-homed operation:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# status peer topology dual-homed
```

The following example shows how to enter template configuration mode and configure the status peer topology for dual-homed operation:

```
Device(config)# template type pseudowire template1  
Device(config-template)# encapsulation mpls  
Device(config-template)# status peer topology dual-homed
```

#### Related Commands

Command	Description
<b>encapsulation (pseudowire)</b>	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
<b>pseudowire-class</b>	Enters pseudowire-class configuration mode.

## sync interval

To specify an interval for the device to exchange Precision Time Protocol synchronization messages, use the **sync interval** command in PTP port configuration mode. To disable a sync interval configuration, use the **no** form of this command.

**sync interval** *interval-value*

**no sync interval** *interval-value*

### Syntax Description

<i>interval-value</i>	<p>Value of the interval at which the device sends sync packets. The intervals are set using log base 2 values, as follows:</p> <ul style="list-style-type: none"><li>• 4—1 packet every 16 seconds</li><li>• 3—1 packet every 8 seconds</li><li>• 2—1 packet every 4 seconds</li><li>• 1—1 packet every 2 seconds</li><li>• 0—1 packet every second</li><li>• -1—1 packet every 1/2 second, or 2 packets per second</li><li>• -2—1 packet every 1/4 second, or 4 packets per second</li><li>• -3—1 packet every 1/8 second, or 8 packets per second</li><li>• -4—1 packet every 1/16 seconds, or 16 packets per second</li><li>• -5—1 packet every 1/32 seconds, or 32 packets per second</li><li>• -6—1 packet every 1/64 seconds, or 64 packets per second</li></ul> <p>The recommended value is -6.</p>
-----------------------	---

**Command Default** The default value is 1.

**Command Modes** PTP port configuration (config-ptp-port)

**Command History**

Release	Modification
15.0(1)S	This command was introduced.

**Examples**

The following example shows how to configure the PTP sync interval:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# sync interval -4
Device(config-ptp-port)# end
```

**Related Commands**

Command	Description
<b>clock-port</b>	Specifies the mode of a PTP clock port.

## template (eoam)

To configure a template for use on Ethernet operations, maintenance, and administration (OAM) interfaces and enter configuration template mode, use the **template (eoam)** command in global configuration mode. To remove the template, use the **no** form of this command.

**template** *template-name*

**no template** *template-name*

### Syntax Description

<i>template-name</i>	String that identifies the template.
----------------------	--------------------------------------

### Command Default

No templates are configured.

### Command Modes

Global configuration (config)

### 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

This command groups parameters that can be applied (bound) to one or more interfaces that share the same OAM characteristics. A benefit of using the **template (eoam)** command is that it helps reduce the overall configuration size by grouping repeating commands and streamlines Ethernet OAM interface configuration.

More than one template can be configured but only one template can be associated with a single Ethernet OAM interface. Commands defined in a template may be overridden by explicitly configuring those commands on the interface in interface configuration mode.

### Examples

The following example shows how to create an OAM template named oam and enter configuration template mode:

```
Device(config)# template oam
Device(config-template)#
```

Related Commands

source template (eoam)	Associates a template to an Ethernet OAM interface.
------------------------	---

## timer (Ethernet ring)

To set the time interval for the guard, hold-off, and Wait-to-Restore (WTR) timers for an Ethernet ring profile, use the **timer** command in Ethernet ring protection profile configuration mode. To change the time intervals, use the **no** form of this command.

**timer** {**guard** *seconds* | **hold-off** *seconds* | **wtr** *minutes*}

**no timer** {**guard** | **hold-off** | **wtr**}

### Syntax Description

<b>guard</b> <i>seconds</i>	Configures the guard interval. The time interval ranges from 10 to 2000 seconds.
<b>hold-off</b> <i>seconds</i>	Configures the hold-off interval. The time interval ranges from 0 to 10 seconds.
<b>wtr</b> <i>minutes</i>	Configures the WTR interval. The time interval ranges from 1 to 12 minutes.

### Command Default

The time intervals are not set.

### Command Modes

Ethernet ring profile configuration (config-erp-profile)

### 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.

### Examples

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

```
Device# configure
Device(config)# ethernet ring g8032 profile profile1
Device(config-erp-profile)# timer hold-off 5
```

# tod

To configure the time of day message format used by the 1PPS interface, use the **tod** command in PTP clock port configuration mode. To remove a time of day configuration, use the **no** form of this command.

**tod** *slot/bay* {**iso8601**| **ubx**| **nmea**| **cisco**| **ntp**} [**delay** *delay-amount*]

**no tod** *slot/bay* {**iso8601**| **ubx**| **nmea**| **cisco**| **ntp**} [**delay** *delay-amount*]

## Syntax Description

<i>slot</i>	Slot of the 1PPS interface.
<i>bay</i>	Bay of the 1PPS interface.
<b>iso8601</b>	Specifies ISO 8601 time of day format.
<b>ubx</b>	Specifies UBX time of day format.
<b>nmea</b>	Specifies NMEA time of day format.
<b>cisco</b>	Specifies Cisco time of day format.
<b>ntp</b>	Specifies NTP time of day format.
<b>delay</b>	(Optional) Specifies a delay between the 1PPS message and the time of day message.
<i>delay-amount</i>	Amount of delay between the 1PPS message and the time of day message, in milliseconds. The range is from 1 to 999.

## Command Default

The time of day message format is not configured.

## Command Modes

PTP clock port configuration (config-ptp-clk)

## Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.



### Usage Guidelines

This command applies only to platforms that have 1PPS ports.

### Examples

The following example shows how to configure a time of day value:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# tod 3/0 ntp
Device(config-ptp-clk)# end
```

This example shows the configuration of the time of (ToD) message format for a 1588V2 Master on a Cisco ASR 901 Series Aggregation Services Router:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# tod 3/0 cisco
Device(config-ptp-clk)# input lpps 3/3
Device(config-ptp-clk)# clock-port MASTER master
Device(config-ptp-clk)# transport ipv4 unicast interface Gi3/3/1 negotiation
Device(config-ptp-clk)# end
```

### Related Commands

Command	Description
<b>input</b>	Enables PTP input clocking using the 1.544 Mhz, 2.048 Mhz, or 10 Mhz timing interface or phase using the 1PPS or RS-422 interface.
<b>output</b>	Enables output of time of day messages using the 1PPS interface.

## traceroute ethernet

To send Ethernet connectivity fault management (CFM) traceroute messages to a destination maintenance endpoint (MEP), use the **traceroute ethernet** command in privileged EXEC mode. This command does not have a **no** form.

**traceroute ethernet** *{mac-address| mpid mpid}* **domain** *domain-name* *{port| service| service-instance identifier|* **icc** *icc-code meg-code|* **number** *maintenance-association-number* *} [cos value] [fdb-only| source mpid]*

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

**traceroute ethernet** *{mac-address| mpid mpid}* **domain** *domain-name* **service** *{short-ma-name|* **icc** *icc-code meg-id|* **number** *ma-number|* **vlan-id** *vlan-id|* **vpn-id** *vpn-id* *} [cos value] [fdb-only| source mpid]*

### Cisco ASR 901 Series Aggregation Services Router

**traceroute ethernet** *mac-address* **domain** *domain-name* *{vlan vlan-id| level level-id}*

#### Syntax Description

<i>mac-address</i>	MAC address of a remote MEP in the format abcd.abcd.abcd.
<b>mpid</b>	Specifies a destination MEP.
<i>mpid</i>	Integer from 1 to 8191 that identifies the MEP.
<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.
<b>cos</b>	(Optional) Specifies a class of service (CoS).

<i>value</i>	(Optional) Integer from 0 to 7 that identifies the CoS.
<b>fdb-only</b>	(Optional) Specifies the forwarding database (FDB) table.
<b>source</b>	(Optional) Specifies a source MEP.
<b>vlan</b>	Specifies a VLAN.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the VLAN.
<b>level</b>	Indicates a maintenance level is specified.
<i>level-id</i>	Integer from 0 to 7 that identifies the maintenance level.

**Command Modes**

Privileged EXEC (#)

**Command History**

Release	Modification
12.2(33)SX12	This command was introduced.
12.2(33)SRE	This command was modified. Support for the <b>evc</b> keyword was added in Cisco IOS Release 12.2(33)SRE.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The <b>service</b> <b>icc</b> keywords were added to provide support for the ICC-based MEG identifier.
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> and <b>evc</b> keywords were deprecated and options to specify the MA service via the <b>service</b> keyword were introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines**

This command does not have a **no** form.

If a CoS is not configured, the default is the highest priority allowed for the egress interface.

FDB is another term for the Layer 2 forwarding table. When the **fdb-only** option is configured, only MAC addresses learned in a bridge's FDB (not information saved in the maintenance intermediate point [MIP] continuity check database [CCDB]) are used to determine the egress port.

The destination can be either a MEP or a MIP. If the destination is a MIP, the FDB must have a MAC address entry for that MIP; that is, the FDB has learned the MIP's MAC address via Linktrace responses.

For a bridge domain-VLAN service, the VLAN ID can be used to initiate traceroute.

On the Cisco Catalyst 6500 series switch, an FDB configuration works only if the origination MEP is a down MEP. Also, for a MEP to clear the Alarm Indication Signal (AIS) defect condition, there should be no corresponding entry in the error database. For example, if you change the remote MEP from an UP MEP to a DOWN MEP, the local entry times out and enters the AIS defect condition. The database starts receiving a new continuity check (CC) entry based on the newly configured DOWN MEP, but the local AIS defect is not yet cleared. It remains in the AIS state until either the archive hold time expires or you issue the **clear ethernet cfm errors** command.

## Examples

The following is sample output from the **traceroute ethernet** command:

```
Device# traceroute ethernet mpid 401 domain Domain_L5 service zzz

Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds
Tracing the route to aabb.cc03.bb99 on Domain Domain_L5, Level 5, service zzz
Traceroute sent via Ethernet0/0.9, path found via MPDB
B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout
-----
  Hops    Host                MAC                Ingress    Ingr Action  Relay Action
        Host                Forwarded    Egress    Egr Action  Previous Hop
-----
! 1                aabb.cc03.bb99
                Not Forwarded                                RlyHit:MEP
                                                aabb.cc03.b999
```

The following example shows the output of the **traceroute ethernet** command for a Cisco ASR 901 Series Aggregation Services Router:

```
Device# traceroute ethernet 10.10.10.10 domain Domain_L5 vlan 9

Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds
Tracing the route to aabb.cc03.bb99 on Domain Domain_L5, Level 5, vlan 9
Traceroute sent via Ethernet0/0.9, path found via MPDB
B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout
-----
  Hops    Host                MAC                Ingress    Ingr Action  Relay Action
        Host                Forwarded    Egress    Egr Action  Previous Hop
-----
! 1                aabb.cc03.bb99
                Not Forwarded                                RlyHit:MEP
                                                aabb.cc03.b999
```

The following table describes the significant fields shown in the display.

**Table 61: traceroute ethernet Field Descriptions**

Field	Description
Hops	Number of hops of the traceroute
Host	Name of the device
MAC	Bridge Brain MAC address of the device
Ingress	Receiving port

Field	Description
Ingr Action	Action on the ingress port: IngOk, IngFilter, IngBlocked
Relay Action	Type of relay action performed: RlyNone, RlyUnknown, RlyFDB, RlyCCDB, RlyFiltered
Forwarded	Traceroute forwarded or not forwarded
Egress	Sending port
Egr Action	Action on the egress port: EgrNone, EgrTTL, EgrDown, EgrBlocked, EgrOk, EgrGVRP, EgrDomainBoundary, EgrFiltered
Previous Hop	MAC address of the neighboring device

**Related Commands**

Command	Description
<b>clear ethernet cfm errors</b>	Removes continuity check error conditions from the error database.
<b>clear ethernet cfm traceroute-cache</b>	Removes the contents of the traceroute cache.
<b>ethernet cfm traceroute-cache</b>	Enables caching of Ethernet CFM data learned through traceroute messages.
<b>show ethernet traceroute-cache</b>	Displays the contents of the traceroute cache.

# tracroute ethernet evc

To send Ethernet connectivity fault management (CFM) traceroute messages to a destination MAC address, use the **tracroute ethernet evc** command in privileged EXEC mode.

**tracroute ethernet** *mac-address* {**domain** *domain-name* {**evc** *evc-name* {**cos** | **fdb-only** | **source**} **port** | **vlan**}}

## Syntax Description

<i>mac-address</i>	MAC address of a remote maintenance endpoint (MEP) in the format abcd.abcd.abcd.
<b>domain</b>	Identifies the domain in which the destination MEP resides.
<i>domain-name</i>	String of a maximum of 154 characters that identifies the domain.
<b>evc</b>	Specifies the Ethernet virtual circuit (EVC) name.
<i>evc-name</i>	String that identifies the EVC name.
<b>cos</b>	Specifies the class-of-service (CoS).
<b>fdb-only</b>	Specifies the use of FDB table only.
<b>source</b>	Specifies the source maintenance point identifier (MPI).
<b>port</b>	Specifies the Down service with no VLAN association.
<b>vlan</b>	Specifies the VLAN ID.

## Command Default

Sends an Ethernet CFM traceroute message to a specified MAC address.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

**Usage Guidelines**

Traceroute messages can be issued only to MEPs. Before you issue the **traceroute ethernet evc** command, you should have an MEP configured for the same EVC and domain.

**Examples**

The following example shows how to send an Ethernet CFM traceroute message to MAC address aabb.cc00.1010 in maintenance level 4 on evc\_100:

```
Router# traceroute ethernet aabb.cc00.1010 level 4 evc evc_100
Type escape sequence to abort. TTL 255. Per-Hop Timeout is 10 seconds
Tracing the route to aabb.cc00.1010 on Domain PROVIDER, Level 4, evc evc_100
Traceroute sent via Ethernet6/0
B = Intermediary Bridge
! = Target Destination
* = Per Hop Timeout
```

Hops	Host	MAC Forwarded	Ingress Egress	Ingress Action Egress Action	Relay Action Next Hop
B 1	PE	aabb.cc00.1011	Et6/0	IngOk	RlyCCDB
		Forwarded	Et1/0.100	EgrOK	CE1
! 2	CE1	aabb.cc00.1010	Et1/0.100	IngOk	RlyNone
		Not Forwarded			

**Related Commands**

Command	Description
<b>clear ethernet cfm traceroute-cache</b>	Removes the contents of the traceroute cache.
<b>ethernet cfm traceroute-cache</b>	Enables caching of Ethernet CFM data learned through traceroute messages.
<b>show ethernet traceroute-cache</b>	Displays the contents of the traceroute cache.
<b>traceroute-ethernet vlan</b>	Sends Ethernet CFM traceroute messages to a destination MAC address.

# traceroute ethernet vlan

To send Ethernet connectivity fault management (CFM) traceroute messages to a destination MAC address, use the **traceroute ethernet vlan** command in privileged EXEC mode.

**traceroute ethernet** *mac-address* [**domain** *domain-name*] [**level** *level-id*] **vlan** *vlan-id*

## Syntax Description

<i>mac-address</i>	MAC address of a remote MEP in the format abcd.abcd.abcd.
<b>domain</b>	Identifies the domain in which the destination MEP resides.
<i>domain-name</i>	String of a maximum of 154 characters that identifies the domain.
<b>level</b>	Indicates the maintenance level where the device with the specified MAC address is located.
<i>level-id</i>	Integer from 0 to 7 that identifies the maintenance level.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the VLAN.

## Command Default

Sends an Ethernet CFM traceroute message to a specified MAC address.

## Command Modes

Privileged EXEC (#)

## 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.
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**

Traceroute messages can be issued only to maintenance endpoints (MEPs). Before you issue the **traceroute ethernet vlan** command, you should have a MEP configured for the same VLAN and domain.

**Examples**

The following example shows how to send an Ethernet CFM traceroute message to MAC address bc12.cc12.dc12 in maintenance level 3, VLAN ID 2550:

```
Device# traceroute ethernet bc12.cc12.dc12 level 3 vlan 2550
```

```
Type escape sequence to abort. TTL 255. Per-Hop Timeout is 10 seconds
Tracing the route to aabb.cc00.0400 on Domain DOMAIN_OPERATOR_L5_1, Level 5, vlan 7
Traceroute sent via Ethernet1/0.6
```

```
-----
Hops  Host                MAC          Ingress Ingress Action  Relay Action
      Forwarded      Egress  Egress Action  Next Hop
-----
B 1   denver          aabb.cc00.0200 Forwarded Et0/0    EgrOK     RlyCCDB
      Forwarded      Egress  Egress Action  Next Hop
! 2   boston          aabb.cc00.0400 Not Forwarded
      Not Forwarded
```

**Related Commands**

Command	Description
<b>clear ethernet cfm traceroute-cache</b>	Removes the contents of the traceroute cache.
<b>ethernet cfm traceroute-cache</b>	Enables caching of Ethernet CFM data learned through traceroute messages.
<b>show ethernet traceroute-cache</b>	Displays the contents of the traceroute cache.

## transport ipv4 (PTP)

To specify the IP version, transmission mode, and interface that a Precision Time Protocol clock port uses to exchange timing packets, use the **transport ipv4** command in PTP clock port configuration mode. To remove a transport configuration, use the **no** form of this command.

**transport ipv4** {unicast| multicast| multicast-mix} **interface** *interface-type* *interface-number* [**negotiation**]

**no transport ipv4** {unicast| multicast| multicast-mix} **interface** *interface-type* *interface-number* [**negotiation**]

### Syntax Description

<b>unicast</b>	Configures the clock port to exchange timing packets in unicast mode.
<b>multicast</b>	Configures the clock port to exchange timing packets in multicast mode.
<b>multicast-mix</b>	Configures the clock port to exchange timing packets in multicast-unicast communication mode. In multicast-unicast mode, the clock port sends initial Announce and Sync messages as multicast; if a slave device responds with a unicast message, the clock port sends the Delay-Resp message as unicast.
<b>interface</b>	Specifies an interface on the device.
<i>interface-type</i>	The type of the interface.
<i>interface-number</i>	The number of the interface.
<b>negotiation</b>	(Optional) Enables dynamic discovery of slave devices and their preferred format for sync interval and announce interval messages.

### Command Default

The IP version, transmission mode, and interface are not specified for exchanging timing packets.

### Command Modes

PTP clock port configuration (config-ptp-clk)

### Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

### Usage Guidelines

You can configure different transport values for each PTP clock port.

### Examples

The following example shows how to use the **transportipv4** command:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port masterport master
Device(config-ptp-clk)# transport ipv4 unicast interface top5/2/2
Device(config-ptp-clk)# end
```

### Related Commands

Command	Description
<b>clock-port</b>	Specifies the mode of a PTP clock port.

# uni count

To set the user-network interface (UNI) count for an Ethernet virtual connection (EVC), use the **uni count** command in EVC configuration mode. To return to the default setting, use the **no** form of this command.

**uni count** *value* [**multipoint**]

**no uni count**

## Syntax Description

<i>value</i>	Integer in the range of 2 to 1024 that is the number of UNIs in the EVC. The default is 2.
<b>multipoint</b>	(Optional) Indicates point-to-multipoint service. This option is available only with a uni count value of 2.

## Command Default

The UNI count defaults to 2 and the service defaults to point-to-point service.

## Command Modes

EVC configuration (config-evc)

## 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

The UNI count determines the type of service in the EVC.

- A UNI count value of 1 or 2--The service defaults to point-to-point service.
- A UNI value of 2--You can leave the service at the default or you can configure point-to-multipoint service by entering the **multipoint** keyword.
- A UNI value of 3 or greater--The service is point-to-multipoint.

You should know the correct number of maintenance end points (MEPs) in the domain. If you enter a UNI count value greater than the number of endpoints, the UNI status shows as partially active even if all endpoints are up. If you enter a UNI count less than the number of endpoints, UNI status shows as active, even if all endpoints are not up.

**Caution**

Configuring a UNI count does not prevent you from configuring more endpoints than the configured number of UNIs. For example, if you configure a UNI count of 5, but you create 10 MEPs, any 5 MEPs in the domain can go down without the status changing to partially active.

**Examples**

The following example shows how to set a UNI count of 2 with point-to-multipoint service:

```
Device(config)# ethernet evc test1
Device(config-evc)# uni count 2 multipoint
```

**Related Commands**

Command	Description
<b>ethernet evc</b>	Defines an EVC and enters EVC configuration mode.

## weight (srvs instance)

To assign a weight to an Ethernet service instance, use the **weight** command in service instance configuration mode. To remove the weight assignment, use the **no** form of this command.

**weight** *weight*

**no weight**

### Syntax Description

<i>weight</i>	Integer from 1 to 10000 that is the weight value. The default is 1.
---------------	---

### Command Default

If a specific weight is not configured, the Ethernet service instance inherits the default weight of 1.

### Command Modes

Service instance configuration (config-if-srv)

### Command History

Release	Modification
15.0(1)S	This command was introduced.

### Usage Guidelines

Performing this command more than once on the same Ethernet service instance overwrites the previously configured weight. To allow for out-of-order configuration, weights may be configured on Ethernet service instances before weighted load balancing is configured on the port channel.

The weight chosen for an Ethernet service instance should be based on the expected amount of traffic to egress the service instance relative to other Ethernet service instances. For example, an Ethernet service instance configured with a weight of 8 is expected to transmit twice the traffic of an Ethernet service instance configured with a weight of 4. The configured weights allow the load-balancing algorithm to more evenly distribute the service instances across the available member links. The **weight** command is optional and if it is not configured, the Ethernet service instance inherits the default weight.

### Examples

The following example shows how to assign a weight of 250 to Ethernet service instance 100:

```
Router(config)# interface port-channel10
Router(config-if)# port-channel load-balance weighted link all
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# weight 250
```

**Related Commands**

Command	Description
<b>port-channel load-balance (interface)</b>	Configures a member link for load balancing, a default Ethernet service instance weight, or weighted load balancing on port-channel member links.

weight (srvs instance)