mac access-group in through show ethernet cfm errors

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

access-list-name	Name of a MAC ACL to apply to an interface or subinterface (as specified by the mac **access-list extended** 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
mac access-list extended	Defines a MAC ACL.
show ethernet service instance	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

seconds	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-bdomain)# 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

maximum-addresses	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
mac security maximum addresses	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

maximum-addresses	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.
aging	(Optional) Sets the aging time of the addresses in the MAC address table.
static	(Optional) Specifies that the mac security **aging time** *aging-time* command is also applicable to permitted MAC addresses. **Note** The **mac security aging time** *aging-time* 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 **mac security aging time** command is also applicable to dynamically learned sticky MAC addresses.
time	(Optional) Sets up the aging-time functionality for the MAC security aging operation.
aging-time	(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. **Note** 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
bridge-domain (service instance)	Binds the service instance to a bridge-domain instance.
encapsulation dot1q	Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.
service instance ethernet	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

mac-addr	The 48-bit static MAC address.
auto-learn	(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. • This keyword is available only for static unicast MAC addresses.
disable-snooping	(Optional) Disables Internet Group Multicast Protocol (IGMP) snooping on the multicast MAC address. • This keyword is available only for IPv4 and IPv6 static multicast MAC addresses.

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)# l2 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

mac-addr	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-mimn)# 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

c-mac-addr	48-bit MAC address of the customer bridge.
b-mac-addr	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

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

Usage Guidelines

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
show running all	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

minutes	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)

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)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2. • In this release the command is supported only in CFM IEEE.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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
show running all	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

id	Integer in the range from 0 to 8191 that forms the maintenance point ID (MPID).
evc-name	String that identifies the Ethernet virtual circuit (EVC).
mac	(Optional) Indicates that the MAC address of the MEP is specified.
mac-address	(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
ethernet cfm domain	Defines a CFM maintenance domain at a particular maintenance level.
ethernet cfm mep crosscheck	Enables cross-checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs.

Command	Description
ethernet cfm mep crosscheck start-delay	Configures the maximum amount of time that a device waits for remote MEPs to come up before the cross-check operation is started.
mep crosscheck mpid vlan	Statically defines a remote MEP within a maintenance domain.
show ethernet cfm maintenance points remote crosscheck	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

id	Integer in the range from 0 to 8191 that forms the maintenance point ID (MPID).
vlan-id	Integer in the range from 1 to 4094 that identifies the VLAN.
mac	(Optional) Indicates that the MAC address of the MEP is specified.
mac-address	(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
ethernet cfm domain	Defines a CFM maintenance domain at a particular maintenance level.
ethernet cfm mep crosscheck	Enables cross-checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs.

Command	Description
ethernet cfm mep crosscheck start-delay	Configures the maximum amount of time that a device waits for remote MEPs to come up before the cross-check operation is started.
show ethernet cfm maintenance points remote crosscheck	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

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

Usage Guidelines

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

lower-mep-only	(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)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 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

lower-mep-only	(Optional) Creates a MIP only if there is a MEP for the service in another domain at the next lower active maintenance domain level.
none	(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)SXI2	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

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_l5 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

group-id	The *group-id* 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
interface port-channel	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

priority-value	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
interface port-channel	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

node-id	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
interchassis group	Configures an interchassis group in interchassis redundancy configuration mode and assigns a group number.
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

mac-address	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
interchassis group	Configures an interchassis group within the interchassis redundancy configuration mode and assigns a group number.
redundancy	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

priority-value	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
interchassis group	Configures an interchassis group in the interchassis redundancy configuration mode and assigns a group number.
redundancy	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

priority	(Optional) Monitors local Tx and Rx counters for loss functionality.
cos-range	(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

instance-id	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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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

cfm	Specifies Connectivity Fault Management (CFM) as the protocol.
svlan	Specifies a service provider VLAN.
svlan-id	Integer in the range of 1 to 4094 that identifies the service provider VLAN.
domain	Specifies a CFM maintenance domain.
domain-name	String of a maximum of 256 characters that identifies the domain.
ldp	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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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 to 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

1pps	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.
slot	Slot of the 1PPS interface.
bay	Bay of the 1PPS interface.
offset	(Optional) Specifies an offset to compensate for a known phase error such as network asymmetry.
offset-value	Amount of offset in nanoseconds. The range is from 0 to 500,000,000.
negative	Specifies a negative offset 1PPS output value.
pulse-width	(Optional) Specifies a pulse width value.
pulse-amount	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.
ns	Specifies a pulse width value in nanoseconds.
us	Specifies a pulse width value in microseconds.
ms	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 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 subordinate 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
input	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

host *destination-host-address*	Specifies the target LDP destination host address of the peer PE device that belongs to the authorization group.
network *destination-network-address destination-network-mask*	Specifies the target LDP destination network address and network mask of the peer PE devices that belong to the authorization group.
vc-id	Virtual circuit (VC) ID of the peer PE device. Valid values are from 1 to 4294967295.
vc-id-range	(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
l2 subscriber	Creates an L2 subscriber authorization group and enters L2 subscriber group mode.
pseudowire (Layer 2)	Defines the maximum and watermark limits for a pseudowires from a peer PE device.
service-policy type control (Layer 2)	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

seconds	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
show running all	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

mac-address	MAC address of the destination MEP in the format abcd.abcd.abcd.
mpid *mpid*	Specifies a MEP identifier (MPID) and value. Range: 1 to 8191.
multicast	Specifies a multicast loopback message.
domain *domain-name*	Specifies the domain where the destination MEP resides. Maximum: 154 characters.
port	Specifies a port MEP.
service	Specifies the maintenance association (MA) within the domain.
short-ma-name	The short-name identifier for the MA service. The domain name and short MA name combined cannot exceed 48 bytes.
icc *icc-code meg-id*	ITU Carrier Code (ICC) (maximum: 6 characters) and unique maintenance entity group (MEG) ID Code (UMC) (maximum: 12 characters).
number *ma-number*	The MA number. Range: 0 to 65535.
vlan-id *vlan-id*	The primary VLAN ID. Range: 1 to 4094.
vpn-id *vpn-id*	The VPN ID. Range: 1 to 32767.

cos *cos-value*	(Optional) Specifies a class of service (CoS) for a MEP that will be sent in Ethernet CFM messages. CoS value range: 0 to 7. • ICC (maximum: 6 characters) and UMC (maximum: 12 characters). • The default is retrieved from the MEP identified by the MPID if the **cos** keyword is not configured. If the **mpid** keyword is not configured, the default is the highest priority on the egress interface.
source *source-mpid*	(Optional) Specifies an MEP's CoS that will be sent in Ethernet CFM messages. Source MPID value range: 1 to 819.
de	(Optional) Specifies whether the packet is drop-eligible. The **de** option is platform-dependent.
pad	(Optional) Specifies padding data type, length, value (TLV) .
data-pattern	(Optional) The data pattern of data TLV in hexadecimal format.
test	(Optional) Specifies test TLV.
pattern-type *pattern-value*	(Optional) Specifies a pattern type for loopback messages, allowing you to use Test TLV in one-line command format. Pattern value for loopback messages: • 0: Null signal without CRC-32 • 1: Null signal with CRC-32 • 2: PRBS 2 (-31) without CRC-32 • 3: PRBS 2 (-31) with CRC-32
validate	(Optional) Specifies that the reply data is validated.
level	Indicates that a maintenance level is specified.
level-id	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)SXI2	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 **service icc** 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.

Release	Modification
Cisco IOS XE Release 3.7S	This command was modified. • Support for ITU-T Y.1731 CFM Test TLV was added. • The **port** keyword was deprecated and options to specify the MA service via the **service** keyword were introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

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).

Field	Description
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-addressmpid*} {**domain** *domain-name* | **level** *level-id*} **evc** *evc-name* [**cos***cos-value*| **source** *mpid*]

Syntax Description

mac-address	MAC address of the remote maintenance point in the format abcd.abcd.abcd.
mpid	Integer from 0 to 8191 that identifies the MEP.
domain	Indicates a domain is specified.
domain-name	String with a maximum of 154 characters that identifies the domain.
level	Indicates that a maintenance level is specified.
level-id	Integer from 0 to 7 that identifies the maintenance level.
evc-name	String that identifies the Ethernet virtual circuit (EVC).
cos *cos-value*	Specifies the class of service (cos) and the value for the cos.Integer from 0 to 7 that identifies the value for cos.
source *mpid*	(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
ping	Sends an echo request packet to an address, and then awaits a reply to determine whether a device can be reached or is functioning.
ping ethernet vlan	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

mpid	Integer from 0 to 8191 that identifies the MEP.
domain	Indicates a domain where the destination MEP resides is specified.
domain-name	String with a maximum of 154 characters that identifies the domain.
level	Indicates a maintenance level is specified.
level-id	Integer from 0 to 7 that identifies the maintenance level.
vlan-id	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 **ping ethernet vlan** 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
ping	Sends an echo request packet to an address, and then awaits a reply to determine whether a device can be reached or is functioning.
ping ethernet vlan	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-addressmpid*} {**domain** *domain-name* | **level** *level-id*} **vlan** *vlan-id* [**source** *mpid*]

Syntax Description

mac-address	MAC address of the remote maintenance point in the format abcd.abcd.abcd.
mpid	Integer from 0 to 8191 that identifies the MEP.
domain	Indicates a domain is specified.
domain-name	String with a maximum of 154 characters that identifies the domain.
level	Indicates that a maintenance level is specified.
level-id	Integer value of 0 to 7 that identifies the maintenance level.
vlan-id	Integer value of 1 to 4094 that identifies the VLAN.
source *mpid*	(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 **source** keyword and *mpid* 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.
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
ping	Sends an echo request packet to an address, and then awaits a reply to determine whether a device can be reached or is functioning.

police match any

This command is used under a specific vrf to help police the egress traffic rate for a VNET. There is a N-to-M mapping between a vrf and vni.There can be multiple VNI instances associated with a VRF, and a single VNI instance can be associated with multiple VRF. The combination of VRF and VNI uniquely identifies an instance.

police match any vni id *vni_id* **rate** *bps_rate*
no police match any vni id *vni_id* **rate** *bps_rate*

Syntax Description

vni_id	Indicates the VXLAN identifier.
bps_rate	Indicates the rate at which traffic is transferred.

Command Modes

VxLAN config VRF policy mode (config-vxlan-route-policy-vrf)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1	This command was introduced.

Examples

This example shows how to use this command:

```
Router(config)# vxlan static-route policy output
Router(config-vxlan-route-policy)# vrf vrf1
Router(config-vxlan-route-policy-vrf)# police match any vni 1 rate 800
Router(config)#
```

Related Commands

Command	Description
vxlan static-route accounting-policying bind p2p-tunnel	You can enable it or disable binding according to business requirement. If you want to count and police the traffic both through VxLAN static route and VxLAN p2p tunnel, use the **vxlan static-route accounting-policying bind p2p-tunnel**.

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

interface *type number*	Interface type and number. Enter the **interface** 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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

This command also enters Ethernet ring 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

instance-id	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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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

interface *type number*	Interface type and number. Enter the **interface** keyword followed by the interface type and interface number.
none	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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

This command also enters Ethernet ring 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

instance-id	Service instance identifier. Valid entries are in the range of 1 to 4000.
none	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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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

method	Load distribution method; see the "Usage Guidelines" section for a list of valid values.
module	Specifies the module on which the load-distribution method is set. This keyword is supported only on DFC systems.
slot	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	This command was modified. The following keywords were added: **dst-mixed-ip-port**, **src-dst-mixed-ip-port**, **src-mixed-ip-port**,and **exclude vlan**. • These keywords are supported on systems that are in PFC3C or PFC3CXL mode (PFC3C or PFC3CXL with no DFC3A or DFC3B/BXL) only. • The **exclude vlan**keyword is added only for IP-related load balance options.
12.2(50)SY	This command was modified. The following methods were added: • **vlan-dst-ip** • **vlan-dst-mixed-ip-port** • **vlan-src-dst-ip** • **vlan-src-dst-mixed-ip-port** • **vlan-src-ip** • **vlan-src-mixed-ip-port** These methods are supported only in Cisco IOS Release12.2(50)SY.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
port-channel load-balance mpls	Sets the load distribution method among the ports in the bundle for MPLS packets.
show etherchannel	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

link	Configures a member link for egress load balancing.
link-id	Integer from 1 to 16 that identifies the member link. • When used with the **weighted** keyword, the *link-id* is a comma-delimited list of member link IDs to use for weighted load balancing.
weighted	Configures weighted load balancing on the port channel.
default weight	Configures a default weight for a service instance.
weight	Integer from 1 to 10000 that is the weight value. The default is 1. • When used with the **rebalance** keyword, this value is the threshold weight used to trigger automatic rebalancing. The default is 4.
all	Configures load balancing across all active member links.
rebalance	Sets or disables the automatic rebalance threshold.
disable	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

label	Specifies using the MPLS label to distribute packets; see the "Usage Guidelines" section for additional information.
label-ip	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
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
show etherchannel	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

interface	(Optional) Specifies a port channel enabled for weighted load balancing.
port-channel	(Optional) Specifies an Ethernet channel of interfaces.
number	(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
port-channel load-balance (interface)	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

priorityvalue	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

Subordinate devices use the priority1 value when selecting a primary 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
priority2	Sets the PTP priority2 value.

priority2

To set a 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

priorityvalue	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

Subordinate devices use the priority2 value to select a primary 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
priority1	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

profile-name	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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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

maximum	Specifies the maximum number of Any Transport over MPLS (AToM) virtual circuits (VCs) allowed to be configured from the peer PE devices.
watermark high	Specifies the high watermark limit for the AToM VCs from the peer PE devices.
limit	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)# l2 subscriber authorization group group1
Router(config-l2-sub-gr)# pseudowire maximum 58
```

Related Commands

Command	Description
l2 subscriber	Creates an L2 subscriber authorization group, and enters L2 subscriber group mode.
peer	Defines the target LDP peer PE information.
service-policy type control (Layer 2)	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

ordinary	Sets the PTP clock to ordinary clocking mode.
transparent	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.
boundary	Sets the PTP clock to boundary clock mode; the router participates in selecting the best primary clock and can act as the primary clock if no better clocks are detected.
domain	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
clock-port	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* | **dot1q** *vlan-id* {**second-dot1q** *vlan-id* | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} **second-dot1q** *vlan-id*}}

no rewrite egress

Syntax Description

pop	Specifies removing a tag.
1	Specifies the outermost tag in a packet.
2	Specifies the two outermost tags in a packet.
push	Adds a tag.
dot1ad	Specifies a dot1ad VLAN tag.
vlan-id	Integer from 1 to 4094 that identifies a VLAN.
dot1q	Specifies a tag with the dot1q Ethertype.
second-dot1q	Specifies a second tag with the dot1q Ethertype.
vlan-type	Specifies type of VLAN protocol.
0x88a8	Specifies VLAN protocol type.
0x9100	Specifies VLAN protocol type.
0x9200	Specifies VLAN protocol type.
translate	Translates a VLAN tag.
1-to-1	Translates a VLAN tag to a different VLAN tag.
1-to-2	Translates a single VLAN tag to two different VLAN tags.
2-to-1	Translates two different VLAN tags to a single VLAN tag.
2-to-2	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)

Command History

Release	Modification
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

pop	Removes a tag from a packet.
{**1** | **2**}	Specifies either the outermost tag or the two outermost tags for removal from a packet.
symmetric	(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.
push	Adds a tag.
dot1ad	Specifies an IEEE 802.1ad tag.
vlan-id	Integer in the range 1 to 4094 that identifies the VLAN.
dot1q	Specifies an IEEE 802.1Q tag.
second-dot1q	Specifies a different 802.1Q tag at the ingress service instance.
vlan-type	Specifies the type of VLAN protocol.
0x88a8	Specifies the protocol type 0x88a8.
0x9100	Specifies the protocol type 0x9100.
0x9200	Specifies the protocol type 0x9200.

translate	Translates, by VLAN ID, a tag or a pair of tags defined in the **encapsulation** command.
1-to-1	Translates a single tag defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command.
1-to-2	Translates a single tag defined by the **encapsulation** command to a pair of tags defined in the **rewrite ingress tag** command.
2-to-1	Translates, by VLAN ID, a pair of tags defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command.
2-to-2	Translates, by VLAN ID, a pair of tags defined by the **encapsulation** command to a pair of tags defined in the **rewrite ingress tag** 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

Release	Modification
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
encapsulation	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

port0	Specifies port0 as the ring port.
port1	Specifies port1 as the ring port.
owner	Specifies the ring port as the RPL owner.
neighbor	Specifies the ring port as the RPL neighbor.
next-neighbor	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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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

chassis	Sends only the chassis ID information.
none	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)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 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-namema-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [{**port** | **vlan** *vlan-id* [**direction down**]}]
no service {*ma-namema-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [{**port** | **vlan** *vlan-id* [**direction down**]}]

Syntax Description

ma-name	Short maintenance association name.
ma-num	Integer from 0 to 65535 that identifies the maintenance association.
vlan-id	Configures a primary VLAN.
vlan-id	Integer from 1 to 4094 that identifies the primary VLAN.
vpn-id	Configures a virtual private network (VPN).
vpn-id	Integer from 1 to 32767 that identifies the VPN.
port	(Optional) Configures a DOWN service direction without a VLAN association.
vlan	(Optional) Configures a VLAN.
direction	(Optional) Configures the service direction. The default is “up.”
down	(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.
Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

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

service	Specifies the service instance.
csi-id	String of a maximum of 100 characters that identifies the CSI.
evc	Specifies the Ethernet virtual circuit (EVC).
evc-name	String that identifies the Ethernet virtual circuit (EVC).
vlan	Specifies the VLAN.
vlan-id	String the VLAN ID. Range is from 1 to 4094.
direction	Specifies the service direction.
down	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
service vlan	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

icc-code	String from 1 to 6 characters that identifies the ITU carrier code.
meg-code	String from 1 to 12 characters that identifies the unique MEG code.
evc	Specifies the Ethernet virtual circuit (EVC).
evc-name	String from 1 to 100 characters that identifies the EVC.
direction down	(Optional) Configures a DOWN service direction.
vlan	(Optional) Configures a primary VLAN.
port	Configures a DOWN service direction without a VLAN association.
vlan-id	Integer from 1 to 4094 that identifies the primary VLAN.
inner-vlan	Specifies the inner VLAN.
inner-vlan-id	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.
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
ethernet cfm domain level	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 **serviceinstancedynamic**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

L2-id	Layer 2 context identifier. Valid values are from 1 to 4000.
ethernet	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 **serviceinstancedynamic** 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
encapsulation dot1q	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
initiator	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

trunk	(Optional) Indicates that the service instance will be configured on a trunk interface.
id	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.
evc-name	(Optional) String that associates an Ethernet virtual connection (EVC) to the service instance. Maximum: 100 bytes.
instance-id	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 **group** command is now available after entering Ethernet service configuration mode.
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 **trunk** 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
ethernet evc	Defines an EVC and enters EVC configuration mode.
ethernet lmi ce-vlan map	Configures Ethernet Local Management Interface parameters.
group (service group)	Adds a member to a service group.

Command	Description
show ethernet service instance	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

id	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

csi-id	String of a maximum of 100 characters that identifies the CSI.
vlan-id	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 **servicepolicytypecontrolpolicy**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

policy-name	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
l2 subscriber	Creates a Layer 2 subscriber authorization group and enters Layer 2 subscriber group mode.
peer	Defines the target LDP peer PE information.
pseudowire (Layer 2)	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

bridge-id	(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.
c-mac	(Optional) Displays a specified customer bridge domain.
mac	(Optional) Displays MAC address data. **Note** The **mac** keyword is not supported on the Cisco ASR 1000 Series Aggregation Services Router.
security	(Optional) Displays MAC security information.
address	(Optional) Displays addresses. • When used with the **security** keyword, displays secure addresses on a specified service instance. • When used with the **static** keyword, displays static addresses in a specified bridge domain. **Note** The **address** keyword is not supported on the Cisco ASR 1000 Series Aggregation Services Router.
last	(Optional) Displays the last violation recorded on the specified bridge domain.
violation	(Optional) Displays information about the last violation recorded on the specified bridge domain.
statistics	(Optional) Displays the number of secured MAC addresses and related statistics.
static	(Optional) Displays static MAC information.
table	(Optional) Displays commands related to the MAC address table.
mac-address	(Optional) Displays the MAC address.
aging-time	(Optional) Displays the time, in minutes, that an entry remains before aging out of the MAC address table.
count	(Optional) Displays the total number of addresses in a bridge-domain table.
split-horizon	(Optional) Displays bridge-domain information for a split-horizon.
group	(Optional) Displays bridge-domain information for a split-horizon group.

group-number	(Optional) Number of a specific split-horizon group for bridge-domain information display.
all	(Optional) Selects all ports in split-horizon groups for bridge-domain information display.
none	(Optional) Selects ports that do not belong to any split-horizon group for bridge-domain information display.
stats	(Optional) Displays bridge-domain statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(33)SRE	This command was modified. The **address**, **aging-time**, **count**, **static**, and **table** keywords and the *mac-address* 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. **Note** 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
clear bridge-domain	Clears bridge-domain attributes that are not needed.
remote command	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.
show ethernet service instance	Displays information about Ethernet service instances.

Command	Description
show ethernet service interface	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

epl	Displays CFM Ethernet private line details.
info	Displays CFM PAL information.
interface	The interface to check the CFM.
type number	The type and the number of the interface. The supported interfaces are FastEthernet, GigabitEthernet, and port channel.
fwd_vlan	Displays the CFM forward VLAN list.
vlan-number	The VLAN number to test the CFM.
level	Displays the CFM level for the interface.
vlan_list	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 cfmpal epl
flowpoint count 0, MCL -2
Router# show cfmpal 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

domain-name	(Optional) String of a maximum length of 154 characters.
brief	(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)SXI2	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.l(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.
Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

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.
Level	Maintenance domain level.
Total Services	Number of services running.
Services	The services currently running.

Field	Description
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
show ethernet cfm maintenance-points remote	Displays information about remote maintenance points in the continuity check database.
show ethernet cfm maintenance-points remote crosscheck	Displays information about remote maintenance points configured statically in a cross-check list.
show ethernet cfm maintenance-points remote detail	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

domain	(Optional) Indicates that a maintenance domain is specified.
domain-name	(Optional) String of a maximum of 154 characters in length.
level	(Optional) Indicates that a maintenance level is specified.
level-id	(Optional) Integer from 0 to 7 that identifies the maintenance level.
configuration	(Optional) Displays the configuration error list information; for example, port, VLAN, and error condition.
domain-id	(Optional) Displays error conditions by domain ID.
domain-name	Number of the Domain. The range is from 0 to 65535.
mac-address	(Optional) MAC address of the maintenance domain.
dns	(Optional) Displays a domain name service (DNS).
dns-name	(Optional) String of a maximum of 43 characters in length.
null	Indicates there is not a domain name.
service	(Optional) Displays a maintenance association within the domain.
icc	(Optional) Displays error conditions by the ITU-T Y.1731 Carrier Code (ICC)-based maintenance entity group (MEG) identifier.
icc-code	(Optional) String that identifies the ICC. String of a maximum length of six characters.
meg-code	(Optional) String that identifies the unique MEG code. String of a maximum length of 12 characters.

maintenance-association-name	(Optional) String that identifies the maintenance association.
number	(Optional) Specifies a maintenance association by a numerical ID.
maintenance-association-number	(Optional) Integer that identifies the maintenance association.
vlan-id	(Optional) Displays a VLAN.
vlan-id	(Optional) Integer from 1 to 4094 that identifies the VLAN.
vpn-id	(Optional) Displays a VPN.
vpn-id	(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.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.
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 **icc** 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.
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.

Field	Description
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
alias	Configures an MA alias within a domain.
show ethernet cfm maintenance-points local	Displays information about maintenance points configured on a device.
show ethernet cfm maintenance-points remote crosscheck	Displays information about remote maintenance points configured statically in a cross-check list.
show ethernet cfm maintenance-points remote detail	Displays information about a remote maintenance point in the continuity check database.

show-macsec-post

To verify the macsec Power on Self Test (POST) configuration, use the **show macsec post** command in privileged EXEC mode.

show macsec post

Command Default

The command is enabled.

Command Mode

Privileged EXEC

Example

To verify the macsec Power on Self Test (POST) configuration:

```
 MACsec Capable Interface                          POST Result
-------------------------------------------------------------
 GigabitEthernet0/1/0                                 PASS
 GigabitEthernet0/1/2                                 PASS
 GigabitEthernet0/1/4                                 PASS
 GigabitEthernet0/1/6                                 PASS
 GigabitEthernet0/1/8                                 NONE
 GigabitEthernet0/1/10                               NONE
 GigabitEthernet0/1/12                               NONE
 GigabitEthernet0/1/14                               NONE
 TenGigabitEthernet0/1/16                          PASS
 GigabitEthernet0/2/0                                  PASS
GigabitEthernet0/2/2                                 PASS
 GigabitEthernet0/2/4                                  PASS
 GigabitEthernet0/2/6                                 NONE
```

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	The command was introduced for ASR 900 and NCS 4206 Cisco RSP3 module.