VPN and Ethernet Services Command Reference for Cisco NCS 5000 Series Routers

First Published: 2015-12-23

Last Modified: 2021-09-01

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

CONTENTS

Preface

This preface contains these sections:

Changes to This Document

This table lists the technical changes made to this document since it was first released.

Table 1: Changes to This Document

Date	Summary
August 2018	Republished with documentation updates for Release 6.5.1 features.
March 2018	Republished with documentation updates for Release 6.3.2 features.
September 2017	Republished with documentation updates for Release 6.3.1 features.
July 2017	Republished with documentation updates for Release 6.2.2 features.
March 2017	Republished with documentation updates for Release 6.2.1 features.
November 2016	Republished with documentation updates for Release 6.1.2 features.
December 2015	Initial release of this document.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Gigabit Ethernet Interfaces Commands

This section describes the commands used to configure Gigabit Ethernet services for Layer 2 VPNs.

For detailed information about concepts and configuration, see the Configure Gigabit Ethernet for Layer 2 VPNs chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5000 Series Routers*.

l2transport (Ethernet)

To enable Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode, use the **l2transport** command in interface or Subinterface configuration mode for an Ethernet interface. To disable Layer 2 transport port mode on an Ethernet interface, use the **no** form of this command.

l2transport
no l2transport

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Sub-interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The l2transport command and these configuration items are mutually exclusive:

- IPv4 address and L3 feature configuration
- IPv4 enable and L3 feature configuration
- Bundle-enabling configuration
- L3 sub-interfaces
- Layer 3 QoS Policy

Note

- After an interface or connection is set to Layer 2 switched, commands such as **ipv4 address** are not usable. If you configure routing commands on the interface, **l2transport** is rejected.
- The **l2transport** command is mutually exclusive with any Layer 3 interface configuration.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode:

```
Router# configure
Router(config)# interface TenGigE 0/2/0/0
Router(config-if)# l2transport
Router(config-if-l2)#
```

Note Ensure that the **l2transport** command is applied on the same line as the **interface** command for the Ethernet sub-interface.

The following example shows how to use the l2transport command on an Ethernet sub-interface:

```
Router# configure
Router(config)# interface TenGigE 0/1/0/3.10 l2transport
Router(config-subif)# encapsulation dot1q 10
```

Examples

The following example shows how to configure an interface or connection as Layer 2 switched under several different modes:

Ethernet Port Mode:

```
Router# configure
Router(config)# interface TenGigE 0/0/0/10
Router(config-if)# l2transport
```

Ethernet VLAN Mode:

```
Router# configure
Router(config)# interface TenGigE 0/0/0/0.1 l2transport
Router(config-if)# encapsulation dot1q 10
```

Ethernet VLAN Mode (QinQ):

```
Router# configure
Router(config)# interface TenGigE 0/0/0/0.1 l2transport
Router(config-if)# encapsulation dot1q 10 second-dot1q 11
```

Note Ensure that the **l2transport** command is applied on the same line as the **interface** command for the Ethernet subinterface.

Related Commands

Command	Description
encapsulation dot1q, on page 7	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 9	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.

flood mode ac-ingress-replication

To add BUM traffic queueing support for attachment circuits in a bridge domain, use the **flood mode ac-ingress-replication** command in the L2VPN bridge group bridge domain configuration mode. To return to the default behavior, use the **no** form of this command.

flood mode ac-ingress-replication

This command has no keywords or arguments.

Command Default

BUM traffic queueing support is not supported for attachment circuits in a bridge domain.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 7.2.1	This command was introduced.
Release 7.2.2	This command was deprecated.

Usage Guidelines

BUM traffic queueing support for attachment circuits in a bridge domain is not supported on devices that have multiple NPUs or line cards. It is only supported on single NPU devices.

Perform this task to add BUM traffic queueing support for attachment circuits in a bridge domain

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 10
Router(config-l2vpn-bg)# bridge-domain 1
Router(config-l2vpn-bg-bd)# flood mode ac-ingress-replication
Router(config-l2vpn-bg-bd)# commit
```

Virtual LAN Commands

This section describes the commands used to configure virtual LANs in Layer 2 VPNs.

For detailed information about concepts and configuration, see the Configure Virtual LANs in Layer 2 VPNs chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5000 Series Routers*.

encapsulation default

To configure the default service instance on a port, use the **encapsulation default** command in the Interface configuration mode. To delete the default service instance on a port, use the **no** form of this command.

encapsulation default

Syntax Description

This command has no keywords or arguments.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

If the default service instance is the only one configured on a port, the **encapsulation default** command matches all ingress frames on that port. If the default service instance is configured on a port that has other non-default service instances, the **encapsulation default** command matches frames that are unmatched by those non-default service instances (anything that does not meet the criteria of other services instances on the same physical interface falls into this service instance).

Only a single default service instance can be configured per interface. If you attempt to configure more than one default service instance per interface, the **encapsulation default** command is rejected.

Only one encapsulation command must be configured per service instance.

Examples

The following example shows how to configure a service instance on a port:

```
Router(config-if)# encapsulation default
```

Related Commands

Command	Description
encapsulation dot1q, on page 7	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1ad dot1q, on page 10	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 9	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.

encapsulation dot1q

To define the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance, use the **encapsulation dot1q** command in the interface configuration mode. To delete the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance, use the **no** form of this command.

encapsulation dot1q *vlan-id* [{**second-dot1q** *vlan-id*}]
no encapsulation dot1q

Syntax Description

vlan-id	VLAN ID, can be given as single ID.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Only one encapsulation statement can be applied to a sub-interface. Encapsulation statements cannot be applied to main interfaces.

A single encapsulation dot1q statement specifies matching for frames with a single VLAN ID.

Examples

The following example shows how to map 802.1Q frames ingress on an interface to the appropriate service instance:

```
Router(config-if)# encapsulation dot1q 10
```

The following example shows how to map 802.1Q frames ingress on an l2transport sub-interface:

```
Router# configure
Router(config)# interface TenGigE 0/1/0/3.10 l2transport
Router(config-subif)# encapsulation dot1q 10
```

Related Commands

Command	Description
encapsulation dot1q second-dot1q, on page 9	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1ad, on page 8	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.
rewrite ingress tag, on page 14	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.

encapsulation dot1ad

To define the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance, use the **encapsulation dot1ad** command in the interface configuration mode. To delete the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance, use the **no** form of this command.

encapsulation dot1ad *vlan-id* [{**second-dot1ad** *vlan-id*}]
no encapsulation dot1ad

Syntax Description

vlan-id	VLAN ID, can be given as single ID.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Only one encapsulation statement can be applied to a sub-interface. Encapsulation statements cannot be applied to main interfaces.

A single encapsulation dot1ad statement specifies matching for frames with a single VLAN ID.

Examples

The following example shows how to map 802.1ad frames ingress on an interface to the appropriate service instance:

```
Router(config-if)# encapsulation dot1ad 10
```

The following example shows how to map 802.1ad frames ingress on an l2transport sub-interface:

```
Router# configure
Router(config)# interface TenGigE 0/1/0/3.10 l2transport
Router(config-subif)# encapsulation dot1ad 10
```

Related Commands

Command	Description
encapsulation dot1q second-dot1q, on page 9	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1q, on page 7	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
rewrite ingress tag, on page 14	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.

encapsulation dot1q second-dot1q

To define the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance, use the **encapsulation dot1q second-dot1q** command in the interface configuration mode. To remove the configuration, use the **no** form of this command.

encapsulation dot1q *vlan-id* [{**second-dot1q** *vlan-id*}]
no encapsulation dot1q *vlan-id* [{**second-dot1q** *vlan-id*}]

Syntax Description

vlan-id	VLAN ID, can be given as single ID.
second-dot1q	(Optional) Specifies IEEE 802.1Q VLAN tagged packets.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The following restrictions are applicable for this command:

- The outer tag must be unique and the inner tag may be a single VLAN.
- QinQ service instance, allows single or multiple on second-dot1q.
- Only one encapsulation command must be configured per service instance.
- Overlapping inner VLAN ranges are not supported.
-

Examples

The following example shows how to map ingress frames to a service instance:

```
Router(config-if)# encapsulation dot1q 10 second-dot1q 20
```

Related Commands

Command	Description
encapsulation dot1q, on page 7	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1ad, on page 8	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.
rewrite ingress tag, on page 14	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.

encapsulation dot1ad dot1q

To define the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance, use the **encapsulation dot1ad dot1q** command in sub-interface configuration mode. To remove the configuration, use the **no** form of this command.

encapsulation dot1ad *vlan-id* **dot1q** *vlan-id*
no encapsulation dot1ad *vlan-id* **dot1q** *vlan-id*

Syntax Description

dot1ad	Indicates that the IEEE 802.1ad provider bridges encapsulation type is used for the outer tag.
dot1q	Indicates that the IEEE 802.1q standard encapsulation type is used for the inner tag.
vlan-id	VLAN ID, can be given as single ID.

Command Default

No matching criteria are defined.

Command Modes

Sub-interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The outer VLAN tag is an 802.1ad VLAN tag, instead of an 802.1Q tag. An 802.1ad tag has an ethertype value of 0x88A8, instead of 0x8100 that 802.1Q uses.

Some of the fields in the 802.1ad VLAN header are interpreted differently per 802.1ad standard.

Examples

The following example shows how to map single-tagged 802.1ad ingress frames to a service instance:

```
Router(config-subif)# encapsulation dot1ad 100 dot1q 20
```

Related Commands

Command	Description
encapsulation dot1q second-dot1q, on page 9	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1ad, on page 8	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.
rewrite ingress tag, on page 14	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.

encapsulation list-extended dot1q

To configure up to 64 VLAN-IDs, either on the outer or on the inner VLAN list, use the **encapsulation list-extended dot1q** command in the interface configuration mode. To remove the VLAN-ID configuration, use the **no** form of this command.

encapsulation list-extended dot1q *vlan-id*
no encapsulation list-extended dot1q *vlan-id*

Syntax Description

vlan-id	VLAN ID, can be given as single ID. A comma-separated list of VLAN ranges in the form a-b, c, d, e-f, g and so on.You can configure up to 64 VLAN-IDs.

Command Default

If encapsulation command is not configured, then no matching criteria is defined for that subinterface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

Do not use both the **encapsulation default** and **encapsulation list-extended** commands, on the same subinterface.

- If you migrate from **encapsulation** command to **encapsulation list-extended** command, then **no encapsulation** command must precede the **encapsulation list-extended** command.
- If you migrate from **encapsulation list-extended** command to **encapsulation** command, then **no encapsulation list-extended** command must precede the **encapsulation** command.

The **encapsulation list-extended dot1q** command supports only comma-separated list of outer and inner VLAN tags or VLAN ranges along with untagged Ethernet frames (no spaces allowed between the tags).

Examples

The following example shows how to configure the maximum number of VLAN IDs, on an L2 subinterface:

```
Router(config)#interface TenGigabitEthernet 0/0/0/1.101 l2transport
Router(config-subif)#encapsulation list-extended dot1q
66-67,68-69,70-71,118-119,120-121,122-123,229,230,231
```

encapsulation untagged

To define the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance, use the **encapsulation untagged** command in the Interface configuration mode. To delete the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance, use the **no** form of this command.

encapsulation untagged [**ingress source-mac** *mac-address*]
no encapsulation untagged

Syntax Description

ingress source-mac	(Optional) Performs MAC-based matching.
mac-address	Specifies the source MAC address.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Only one service instance per port is allowed to have untagged encapsulation. The reason is to be able to unambiguously map the incoming frames to the service instance. However, it is possible for a port that hosts an service instance matching untagged traffic to host other service instances that match tagged frames. Only one encapsulation command may be configured per service instance.

Only one subinterface may be configured as encapsulation untagged. This interface is referred to as the untagged subinterface or untagged EFP (incase of an L2 interface).

The untagged subinterface has a higher priority than the main interface; all untagged traffic, including L2 protocol traffic, passes through this subinterface rather than the main interface. If the **ethernet filtering** command is applied to a main interface having an untagged subinterface, the filtering is applied to the untagged subinterface.

Examples

The following example shows how to map untagged ingress Ethernet frames to a service instance:

Example 1:

```
Router# configure
Router(config-if)# encapsulation untagged
```

Example 2:

```
Router# configure
```

```
Router(config)# interface GigabitEthernet 0/1/1/0.100 l2transport
Router(config-subif)# encapsulation untagged
```

Related Commands

Command	Description
encapsulation default, on page 6	Configure the default service instance on a port.
encapsulation dot1q, on page 7	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 9	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.

rewrite ingress tag

To specify the encapsulation adjustment that is to be performed on the frame ingress to the service instance, use the **rewrite ingress tag** command in the interface configuration mode. To delete the encapsulation adjustment that is to be performed on the frame ingress to the service instance, use the **no** form of this command.

rewrite ingress tag {**push** {**dot1q** *vlan-id*} | **pop** {**1**} | **translate** {**1-to-1** {**dot1q** *vlan-id*} | **1-to-2** {**dot1q** *vlan-id* } | **2-to-2** {**dot1q** *vlan-id* **dot1q** *vlan-id*} | **2-to-1 dot1q** *vlan-id*}} [**symmetric**]
no rewrite ingress tag {**push** {**dot1q** *vlan-id*} | **pop** {**1**} | **translate** {**1-to-1** {**dot1q** *vlan-id*} | **1-to-2** {**dot1q** *vlan-id* } | **2-to-2** {**dot1q** *vlan-id* **dot1q** *vlan-id*} | **2-to-1 dot1q** *vlan-id*}} [**symmetric**]

Syntax Description

vlan-id	VLAN ID, can be given as single ID.
push dot1q *vlan-id*	Pushes one 802.1Q tag with *vlan-id*.
pop {1}	One tag is removed from the packet. This command can be combined with a push (pop N and subsequent push *vlan-id*).
translate 1-to-1 dot1q *vlan-id*	Replaces the incoming tag (defined in the encapsulation command) into a different 802.1Q tag at the ingress service instance.
translate 1-to-2 dot1q *vlan-id* **dot1q** *vlan-id*	Replaces the incoming tag defined by the encapsulation command by a pair of 802.1Q tags.
translate 2-to-2 dot1q *vlan-id* **second-dot1q** *vlan-id*	Replaces the pair of tags defined by the encapsulation command by a pair of VLANs defined by this rewrite.
translate 2-to-1 dot1q *vlan-id*	Replaces a pair of tags defined in the **encapsulation** command by vlan-id.
symmetric	(Optional) A rewrite operation is applied on both ingress and egress. The operation on egress is the inverse operation as ingress. **Note** Symmetric is the default behavior. Hence, it cannot be disabled.

Command Default

The frame is left intact on ingress.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **symmetric** keyword is accepted only when a single VLAN is configured in encapsulation. If a list of VLANs is configured in encapsulation, the **symmetric** keyword is accepted only for push rewrite operations; all other rewrite operations are rejected.

The **pop** command assumes the elements being popped are defined by the encapsulation type.

The **rewrite ingress tag translate**command assume 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 “from” tag in the original packet. If the original packet contains more tags than the ones defined in the “from”, then the operation should be done beginning on the outer tag.

Examples

The following example shows how to specify the encapsulation adjustment that is to be performed on the frame ingress to the service instance:

```
Router(config-if)# rewrite ingress tag push dot1q 200
```

Related Commands

Command	Description
encapsulation dot1q, on page 7	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1ad, on page 8	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 9	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1ad dot1q, on page 10	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.

Point-to-Point Layer 2 Services Commands

This section describes the commands used to configure point-to-point services for Layer 2 VPNs.

For detailed information about concepts and configuration, see the Configure Point-to-Point Layer 2 Services chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5000 Series Routers*

.

interface (p2p)

To configure an attachment circuit, use the **interface** command in p2p configuration submode. To return to the default behavior, use the **no** form of this command.

interface *type interface-path-id* **l2transport**
no interface *type interface-path-id* **l2transport**

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

None

Command Modes

p2p configuration sub-mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how you can configure an attachment circuit on a TenGigE interface:

```
Router# configure
Router(config)# interface TenGigE 0/0/0/10.20 l2transport
Router(config-subif)# encapsulation dot1ad 3000
Router(config-subif)# commit
Router(config-subif)#
```

Related Commands

Command	Description
l2transport (Ethernet), on page 2	Enables Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode.

Command	Description
encapsulation dot1ad, on page 8	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.

backup (L2VPN)

To configure the backup pseudowire for the cross-connect, use the **backup** command in L2VPN xconnect p2p pseudowire configuration mode. To disable this feature, use the **no** form of this command.

backup neighbor *IP-address* **pw-id** *value*
no backup neighbor *IP-address* **pw-id** *value*

Syntax Description

neighbor *IP-address*	Specifies the peer to cross connect. The *IP-address* argument is the IPv4 address of the peer.
pw-id *value*	Configures the pseudowire ID. The range is from 1 to 4294967295.

Command Default

None

Command Modes

L2VPN xconnect p2p pseudowire configuration

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

Use the **backup** command to enter L2VPN xconnect p2p pseudowire backup configuration mode.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure backup pseudowires:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group gr1
Router(config-l2vpn-xc)# p2p p001
Router(config-l2vpn-xc-p2p)# neighbor 10.0.0.1 pw-id 2
Router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
```

Related Commands

Command	Description
neighbor (L2VPN), on page 30	Configures a pseudowire for a cross-connect.
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
xconnect group, on page 69	Configures cross-connect groups.

dynamic-arp-inspection

To validate Address Resolution Protocol (ARP) packets in a network, use the **dynamic-arp-inspection** command in the l2vpn bridge group bridge domain configuration mode. To disable dynamic ARP inspection, use the **no** form of this command.

dynamic-arp-inspection {**logging** | **address-validation** {*src-macdst-macipv4*}}

Syntax Description

logging	(Optional) Enables logging. **Note** When you use the logging option, the log messages indicate the interface on which the violation has occured along with the IP or MAC source of the violation traffic. The log messages are rate limited at 1 message per 10 seconds. **Caution** Not all the violation events are recorded in the syslog.
address-validation	(Optional) Performs address-validation.
src-mac	Source MAC address in the Ethernet header.
dst-mac	Destination MAC address in the Ethernet header.
ipv4	IP addresses in the ARP body.

Command Default

Dynamic ARP inspection is disabled.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to enable dynamic ARP inspection on bridge bar:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
```

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

This example shows how to enable dynamic ARP inspection logging on bridge bar:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection logging
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

This example shows how to enable dynamic ARP inspection address validation on bridge bar:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection address-validation
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

hw-module loadbalancing gtp enable

To enable the GPRS Tunneling Protocol (GTP) load balancing for IP traffic, use the **hw-module loadbalancing gtp enable** command in the Global Configuration mode. To disable the feature, use the no form of this command.

hw-module loadbalancing gtp enable

Syntax Description

This command has no arguments or keywords.

Command Default

The load-balancing mode is disabled by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable GTP load balancing for IP traffic:

```
Router# configure
Router(config)# hw-module loadbalancing gtp enable
Router(config)# commit
```

hw-module storm-control-combine-policer-bw

To increase the storm control policer scale per NPU core, use the **hw-module storm-control-combine-policer-bw** command in the global configuration mode. To disable storm control, use the **no** form of this command.

hw-module storm-control-combine-policer-bw enable

Command Default

Storm control combine is disabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 7.4.1	This command was introduced for Cisco NC57 line cards.
Release 7.8.1	This command was modified to support storm control configuration per subinterface.

Usage Guidelines

You must manually reload the router to activate the **hw-module storm-control-combine-policer-bw enable** command.

Examples

The following example activates the combined policer mode:

```
Router# configure
Router#(config)# hw-module storm-control-combine-policer-bw enable
Router# commit
```

The following example shows storm control configuration per subinterface:

```
Router# configure
Router(config)# hw-module storm-control-combine-policer-bw enable
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# interface HundredGigE0/0/0/1.10
Router(config-l2vpn-bg-bd-ac)# storm-control unknown-unicast pps 500
Router(config-l2vpn-bg-bd-ac)# storm-control multicast pps 2000
Router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 1000
Router(config-l2vpn-bg-bd-ac)# commit
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# interface HundredGigE0/0/0/1.20
Router(config-l2vpn-bg-bd-ac)# storm-control unknown-unicast pps 200
Router(config-l2vpn-bg-bd-ac)# storm-control multicast pps 1000
Router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 2000
Router(config-l2vpn-bg-bd-ac)# commit
Router(config-l2vpn-bg-bd-ac)# exit
```

ip-source-guard

To enable source IP address filtering on a layer 2 port, use the **ip-source-guard** command in l2vpn bridge group bridge domain configuration mode. To disable source IP address filtering, use the **no** form of this command.

ip-source-guard logging

Syntax Description

logging	(Optional) Enables logging.

Command Default

IP Source Guard is disabled.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to enable ip source guard on bridge bar:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# ip-source-guard
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ipsg)#
```

This example shows how to enable ip source guard logging on bridge bar:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# ip-source-guard logging
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ipsg)#
```

l2vpn

To enter L2VPN configuration mode, use the **l2vpn** command in the Global Configuration mode. To return to the default behavior, use the **no** form of this command.

l2vpn
no l2vpn

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enter L2VPN configuration mode:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)#
```

l2vpn switchover

To force a manual pseudowire switchover, use the **l2vpn switchover** command in EXEC mode.

l2vpn switchover xconnect neighbor *IP-address* **pw-id** *value*

Syntax Description

xconnect	Configures the switchover for the cross-connect.
neighbor *IP-address*	Configures the peer for the cross-connect.
pw-id *value*	Configures the pseudowire ID. The range is from 1 to 4294967295.

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines If the backup exists, you can switch a primary router over to the backup router. You can use the **l2vpn switchover** command to reactivate the primary router.

Task ID

Task ID	Operations
l2vpn	read, write

Examples The following example shows how to switch a primary pseudowire to a backup pseudowire:

```
Router# l2vpn switchover xconnect neighbor 10.0.0.1 pw-id 2
```

mac secure

To configure MAC security at a port and to set the action that is to be taken when security is violated, use the **mac secure** command in the L2VPN bridge-group, bridge-domain configuration mode or in the EVPN configuration mode.

To configure MAC security in the L2VPN bridge-group, bridge-domain configuration mode use:

mac secure { **action** [{ **none** | **shutdown** }] | **logging** | **threshold** | **shutdown-recovery-timeout** *timer-value* }

Syntax Description

action	(Optional) Indicates the action to be taken when security is violated.
none	Forwards the violating packet and allows the MAC address to be relearned.
shutdown	Shuts down the violating bridge port.
logging	(Optional) Enables logging.
threshold	Enables threshold based mac secure.
shutdown-recovery-timeout *timer-value*	Sets the Recovery timer to revert shutdown action automatically after the timer expires. Recovery timer value can be set in the range of 10 to 3600 seconds.

To configure MAC security in the EVPN configuration mode use:

mac secure [**freeze-time** *freeze-time* | **move-count** *move-count* | **move-interval** *move-interval* | **retry-count** *retry-count* | | **reset-freeze-count-interval** *interval*] **disable**

Syntax Description

freeze-time *freeze-time*	Length of time to lock the MAC address after it has been detected as duplicate. Default is 30 seconds.
move-count *move-count*	Number of moves to occur witin the specified **move-interval** before freezing the MAC address. Default is 5.
move-interval *move-interval*	Interval to watch for subsequent MAC moves before freezing the MAC address. Default is 180 seconds.
retry-count *retry-count*	Number of times to unfreeze a MAC address before freezing it permanently. Default is three times.
reset-freeze-count-interval *interval*	Interval after which the count of duplicate detection events is reset. Default is 24 hours. The range is from is 1 hour to 48 hours.
disable	Disable duplicate detection of MAC address.

Command Default

None

Command Modes

L2VPN bridge-group, bridge-domain configuration

EVPN configuration

Command History

Release	Modification
Release 7.5.1	This command was introduced.

Usage Guidelines

MAC secure is supported on physical and bundle AC, PW, and EVPN.

Task ID

Task ID	Operations
l2vpn	Read, write

Examples

This example shows how to enable MAC security in the L2VPN bridge-group, bridge-domain configuration mode.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge-group BG1
Router(config-l2vpn-bg)# bridge-domain BD1
Router(config-l2vpn-bg-bd)# mac secure
Router(config-l2vpn-bg-bd-mac-sec)# action shutdown
Router(config-l2vpn-bg-bd-mac-sec)# threshold
Router(config-l2vpn-bg-bd-mac-sec)# shutdown-recovery-timeout 300
Router(config-l2vpn-bg-bd-mac-sec)# exit
Router(config-l2vpn-bg-bd)# interface GigabitEthernet0/2/0/0.1
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# interface GigabitEthernet0/2/0/0.2
Router(config-l2vpn-bg-bd-ac)# commit
```

Examples

This example shows how to enable MAC security in the EVPN configuration mode.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# mac secure
Router(config-evpn-mac-secure)# move-count 7
Router(config-evpn-mac-secure)# move-interval 30
Router(config-evpn-mac-secure)# commit
```

neighbor (L2VPN)

To configure a pseudowire for a cross-connect, use the **neighbor** command in p2p configuration submode. To return to the default behavior, use the **no** form of this command.

neighbor *A.B.C.D*{*A.B.C.D* | **ipv4** *ipv4 address*} **pw-id** *value* [{**backup** | **mpls** | **pw-class** }]
no neighbor *A.B.C.D*{*A.B.C.D* | **ipv4** *ipv4 address*} **pw-id** *value* [{**backup** | **mpls** | **pw-class** }]

Syntax Description

A.B.C.D	IP address of the cross-connect peer.
ipv4 *ipv4 address*	Assigns the IPv4 address of the cross-connect peer.
pw-id *value*	Configures the pseudowire ID and ID value. Range is 1 to 4294967295.
backup	(Optional) Specifies the backup pseudowire for the cross-connect.
mpls	(Optional) Configures an MPLS static label.
pw-class	(Optional) Configures the pseudowire class template name to use for this cross-connect.

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

A cross-connect may have two segments:

1. An Attachment Circuit (AC)
2. An second AC or a pseudowire

Note The pseudowire is identified by two keys: neighbor and pseudowire ID. There may be multiple pseudowires going to the same neighbor. It is not possible to configure only a neighbor.

All L2VPN configurations can be deleted using the **no l2vpn** command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows a point-to-point cross-connect configuration (including pseudowire configuration):

```
Router# configure
Router(config)# l2vpn xconnect group l2vpn
Router(config-l2vpn-xc)# p2p rtrA_to_rtrB
Router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000 pw-class class12
Router(config-xc-p2p)# neighbor 10.1.1.3 pw-id 1001 pw-class class13
Router(config-xc)# p2p rtrC_to_rtrD
Router(config-xc-p2p)# neighbor 10.2.2.3 pw-id 200 pw-class class23
Router(config-xc-p2p)# neighbor 10.2.2.4 pw-id 201 pw-class class24
```

This example shows a point-to-point cross-connect configuration (including pseudowire configuration):

```
Router# configure
Router(config)# l2vpn xconnect group l2vpn
Router(config-l2vpn-xc)# p2p rtrA_to_rtrB
Router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000 pw-class foo
Router(config-xc)# p2p rtrC_to_rtrD
Router(config-xc-p2p)# neighbor 20.2.2.3 pw-id 200 pw-class bar1
```

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
xconnect group, on page 69	Configures cross-connect groups.

p2p

To configure point-to-point cross-connects and to enter p2p configuration submode, use the **p2p** command in L2VPN xconnect mode. To return to the default behavior, use the **no** form of this command.

p2p *xconnect-name*
no p2p *xconnect-name*

Syntax Description

xconnect-name	(Optional) Configures the name of the point-to-point cross- connect.

Command Default

None

Command Modes

L2VPN xconnect

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The name of the point-to-point cross-connect string is a free format description string.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows a point-to-point cross-connect configuration:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p XCON1_P2P3
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/0
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/8
Router(config-l2vpn-xc-p2p)# commit
```

pw-class (L2VPN)

To enter pseudowire class sub-mode to define a pseudowire class template, use the **pw-class** command in L2VPN configuration sub-mode. To delete the pseudowire class, use the **no** form of this command.

pw-class *class-name*
no pw-class *class-name*

Syntax Description

class-name	Pseudowire class name.

Command Default

None

Command Modes

L2VPN configuration sub-mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Note All L2VPN configurations can be deleted using the **no l2vpn** command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to define a simple pseudowire class:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group l1vpn
Router(config-l2vpn-xc)# p2p rtrA_to_rtrB
Router(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
Router(config-l2vpn-xc-p2p-pw)# pw-class kanata01
Router(config-l2vpn-xc-p2p-pw)# encapsulation mpls
Router(config-l2vpn-xc-p2p-pw)# exit
Router(config-l2vpn-xc-p2p)# exit
Router(config-l2vpn)# commit
```

Related Commands

Command	Description
interface (p2p), on page 18	Configures an attachment circuit.
l2vpn, on page 26	Enters L2VPN configuration mode.

Command	Description
show l2vpn, on page 37	Displays L2VPN information
show l2vpn xconnect, on page 62	Displays brief information on configured cross-connects.
show l2vpn pw-class, on page 65	Displays L2VPN pseudowire class information.

pw-class encapsulation mpls

To configure MPLS pseudowire encapsulation, use the **pw-class encapsulation mpls** command in L2VPN pseudowire class configuration mode. To undo the configuration, use the **no** form of this command.

pw-class *class-name* **encapsulation mpls** {**control word** | **ipv4** | **load-balancingflow-label** | **preferred-path** | **protocol ldp** | **redundancy one-way** | **sequencing** | **tag-rewrite** | **transport-mode** | **vccv verification-type none**}
no pw-class *class-name* **encapsulation mpls** {**control word** | **ipv4** | **load-balancing**`flow-label` | **preferred-path** | **protocol ldp** | **redundancy one-way** | **sequencing** | **tag-rewrite** | **transport-mode** | **vccv verification-type none**}

Syntax Description

class-name	Encapsulation class name.
control word	Disables control word for MPLS encapsulation. Disabled by default.
ipv4	Sets the local source IPv4 address.
load-balancing flow-label	Sets flow label-based load balancing.
preferred-path	Configures the preferred path tunnel settings.
protocol ldp	Configures LDP as the signaling protocol for this pseudowire class.
redundancy one-way	Configures one-way PW redundancy behavior in the Redundancy Group.
sequencing	Configures sequencing on receive or transmit.
tag-rewrite	Configures VLAN tag rewrite.
transport-mode	Configures transport mode to be Ethernet. The transport-mode VLAN is not suppported.
vccv none	Enables or disables the VCCV verification type.

Command Default

None

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Note All L2VPN configurations can be deleted using the **no l2vpn** command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to define MPLS pseudowire encapsulation:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# pw-class kanata01
Router(config-l2vpn-pwc)# encapsulation mpls
```

Related Commands

Command	Description
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.

show l2vpn

To display L2VPN information, use the **show l2vpn** command in the EXEC mode.

show l2vpn

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

The following example displays output for the **show l2vpn** command. The output provides an overview of the state of the globally configured features.

```
Router# show l2vpn

Mon Oct 12 14:14:48.869 UTC
HA role     : Active
ISSU role   : Primary
Process FSM : PrimaryActive
---------------------------
PW-Status: enabled
PW-Grouping: disabled
Logging PW: disabled
Logging BD state changes: disabled
Logging VFI state changes: disabled
Logging NSR state changes: disabled
TCN propagation: disabled
PW OAM transmit time: 30s
```

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.

Command	Description
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.

show l2vpn collaborators

To display information about the state of the interprocess communications connections between l2vpn_mgr and other processes, use the **show l2vpn collaborators** command in EXEC mode.

show l2vpn collaborators

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows sample output for the **show l2vpn collaborators** command:

```
Router# show l2vpn collaborators
Mon Oct 12 14:14:57.373 UTC

L2VPN Collaborator stats:
Name                 State       Up Cnts      Down Cnts
-------------------  ----------  -----------  -----------
                 LSD          Up            1            0
```

This table describes the significant fields shown in the display.

Table 2: show l2vpn collaborators Field Descriptions

Field	Description
Name	Abbreviated name of the task interacting with l2vpn_mgr.
State	Indicates if l2vpn_mgr has a working connection with the other process.
Up Cnts	Number of times the connection between l2vpn_mgr and the other process has been successfully established.

Field	Description
Down Cnts	Number of times that the connection between l2vpn_mgr and the other process has failed or been terminated.

Related Commands

Command	Description
show l2vpn, on page 37	Displays L2VPN information

show l2vpn bridge-domain (VPLS)

To display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains, use the **show l2vpn bridge-domain** command in XR EXEC mode.

show l2vpn bridge-domain [{**autodiscovery** | **bd-name** *bridge-domain-name* | **brief** | **detail** | **group** *bridge-domain-group-name* | **hardware** | **interface** *type interface-path-id* | **pw-id** *value* }] **neighbor IP-address** [{**pw-id** *value* | **pbb** | **summary**}]

Syntax Description

autodiscovery	(Optional) Displays BGP autodiscovery information.
bd-name *bridge-domain-name*	(Optional) Displays filter information on the *bridge-domain-name*. The *bridge-domain-name* argument is used to name a bridge domain.
brief	(Optional) Displays brief information about the bridges.
detail	(Optional) Displays detailed information about the bridges. Also, displays the output for the Layer 2 VPN (L2VPN) to indicate whether or not the MAC withdrawal feature is enabled and the number of MAC withdrawal messages that are sent or received from the pseudowire.
group *bridge-domain-group-name*	(Optional) Displays filter information on the bridge-domain group name. The *bridge-domain-group-name* argument is used to name the bridge domain group.
hardware	(Optional) Displays hardware information.
interface *type interface-path-id*	(Optional) Displays the filter information for the interface on the bridge domain. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
neighbor *ip-address*	(Optional) Displays the bridge domains that contain the pseudowires to match the filter for the neighbor. The *ip-address* argument is used to specify IP address of the neighbor.
pw-id *value*	(Optional) Displays the filter for the pseudowire ID. The range is from 1 to 4294967295.
pbb	(Optional) Displays provider backbone bridge information.
summary	(Optional) Displays the summary information for the bridge domain.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification

Usage Guidelines

Use the **interface** keyword to display only the bridge domain that contains the specified interface as an attachment circuit. In the sample output, only the attachment circuit matches the filter that is displayed. No pseudowires are displayed.

When an SR policy is configured as the preferred path for a VPLS circuit, the traffic traverses through the SR policy path. The PW counters are updated with statistics about packets transmitted and received. When the SR policy configuration is deleted, the traffic session is still functional because the traffic transmission switches back to the normal LSP path between the PEs. There is no drop in the end-to-end traffic transmitted. However, the packet statistics counters are reset and start from zero. This is because, when the SR policy is deleted, the PW too gets deleted and the statistics information associated with the old PW is cleared. The counter restarts from zero when the new PW is created after the switch takes place.

Task ID

Task ID	Operations
l2vpn	read

Examples

This is the sample output for **show l2vpn bridge-domain** command.

```
RP/0/RP0/CPU0:router# show l2vpn bridge-domain bd-name evpn detail
Fri Dec 11 06:58:17.691 UTC
Legend: pp = Partially Programmed.
Bridge group: evpn-aa-irb-inter, bridge-domain: evpn, id: 1797, state: up, ShgId: 0, MSTi:
 0
  Coupled state: disabled
  VINE state: EVPN-IRB
  MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw for Access PW: enabled
    MAC withdraw sent on: bridge port up
    MAC withdraw relaying (access to access): disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 64000, Action: none, Notification: syslog
  MAC limit reached: no, threshold: 99%
  MAC port down flush: enabled
  MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
  Dynamic ARP Inspection: disabled, Logging: disabled
  IP Source Guard: disabled, Logging: disabled
  DHCPv4 Snooping: disabled
  DHCPv4 Snooping profile: none
  IGMP Snooping: disabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
  Storm Control: disabled
  Bridge MTU: 1500
  MIB cvplsConfigIndex: 1798
  Filter MAC addresses:
  P2MP PW: disabled
  Multicast Source: Not Set
  Create time: 11/12/2020 02:02:56 (04:55:20 ago)
  No status change since creation
  ACs: 2 (2 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of EVPNs:
    EVPN, state: up
```

```
      evi: 2001
      XC ID 0x800006a7
     Statistics:
       packets: received 0 (unicast 0), sent 0
       bytes: received 0 (unicast 0), sent 0
       MAC move: 0
  List of ACs:
    AC: BVI10001, state is up
      Type Routed-Interface
      MTU 2000; XC ID 0x80000fa3; interworking none
      BVI MAC address:
        0088.0088.0088
      Split Horizon Group: Access
      PD System Data: AF-LIF-IPv4: 0x00000000  AF-LIF-IPv6: 0x00000000 FRR-LIF: 0x00000000

    AC: Bundle-Ether30001.2001, state is up
      Type VLAN; Num Ranges: 1
      Outer Tag: 3001
      Rewrite Tags: []
      VLAN ranges: [2001, 2001]
      MTU 1500; XC ID 0xa00005e0; interworking none; MSTi 1
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 64000, Action: none, Notification: syslog
      MAC limit reached: no, threshold: 99%
      MAC port down flush: enabled
      MAC Secure: disabled, Logging: disabled
      Split Horizon Group: none
      E-Tree: Root
      Dynamic ARP Inspection: disabled, Logging: disabled
      IP Source Guard: disabled, Logging: disabled
      DHCPv4 Snooping: disabled
      DHCPv4 Snooping profile: none
      IGMP Snooping: disabled
      IGMP Snooping profile: none
      MLD Snooping profile: none
      Storm Control: bridge-domain policer
      Static MAC addresses:
      Statistics:
        packets: received 404672709 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 0
        bytes: received 30835628366 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 0
        MAC move: 0
      Storm control drop counters:
        packets: broadcast 0, multicast 0, unknown unicast 0
        bytes: broadcast 0, multicast 0, unknown unicast 0
      Dynamic ARP inspection drop counters:
        packets: 0, bytes: 0
      IP source guard drop counters:
        packets: 0, bytes: 0
      PD System Data: AF-LIF-IPv4: 0x00018919  AF-LIF-IPv6: 0x0001891a FRR-LIF: 0x00000000

  List of Access PWs:
  List of VFIs:
  List of Access VFIs:
```

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.

Command	Description
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information

show l2vpn database

To display L2VPN database, use the **show l2vpn database** command in EXEC mode.

show l2vpn database {**ac** | **node**}

Syntax Description

ac	Displays L2VPN Attachment Circuit (AC) database
node	Displays L2VPN node database.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Even when xSTP (extended spanning tree protocol) operates in the PVRST mode, the output of the show or debug commands flag prefix is displayed as MSTP or MSTi, instead of PVRST.

Task ID

Task ID	Operation
l2vpn	read

The following example displays output for the **show l2vpn database ac** command:

```
Router# show l2vpn database ac

Mon Oct 12 14:15:47.731 UTC
Bundle-Ether1:
      Other-Segment MTU: 0
      Other-Segment status flags: 0x3
      Signaled capability valid: Yes
      Signaled capability flags: 0x360018
      Configured capability flags: 0x0
      XCID: 0xa0000001
      PSN Type: Undefined
      ETH data:
          Xconnect tags: 0
          Vlan rewrite tag: 0
    AC defn:
        ac-ifname: Bundle-Ether1
        capabilities: 0x00368079
        extra-capabilities: 0x00000000
        parent-ifh: 0x00000000
        ac-type: 0x04
        interworking: 0x00
    AC info:
        seg-status-flags: 0x00000003
        segment mtu/l2-mtu: 1500/1514
```

```
TenGigE0/0/0/0.1:
      Other-Segment MTU: 0
      Other-Segment status flags: 0x3
      Signaled capability valid: Yes
      Signaled capability flags: 0x360018
      Configured capability flags: 0x0
      XCID: 0xea
      PSN Type: Undefined
      ETH data:
          Xconnect tags: 0
          Vlan rewrite tag: 0
    AC defn:
        ac-ifname: TenGigE0_0_0_0.1
        capabilities: 0x00368079
        extra-capabilities: 0x00000000
        parent-ifh: 0x08000018
        ac-type: 0x15
        interworking: 0x00
    AC info:
        seg-status-flags: 0x00000003
        segment mtu/l2-mtu: 1504/1518
```

The following example displays output for the **show l2vpn database node** command:

```
Router# show l2vpn database node
Mon Oct 12 14:16:30.540 UTC
Node ID: 0x1000 (0/RP0/CPU0)
   MA: vlan_ma      inited:1, flags:0x 2, circuits:3744
     AC event trace history [Total events: 4]
     ----------------------------------------
     Time                Event                          Num Rcvd    Num Sent
     ====                =====                          ========    ========
     10/12/2015 12:46:00 Process joined                 0           0
     10/12/2015 12:46:00 Process init success           0           0
     10/12/2015 12:46:00 Replay start rcvd              0           0
     10/12/2015 12:46:00 Replay end rcvd                0           0

   MA: ether_ma     inited:1, flags:0x 2, circuits:2
     AC event trace history [Total events: 4]
     ----------------------------------------
     Time                Event                          Num Rcvd    Num Sent
     ====                =====                          ========    ========
     10/12/2015 12:41:19 Process joined                 0           0
     10/12/2015 12:41:19 Process init success           0           0
     10/12/2015 12:41:19 Replay start rcvd              0           0
     10/12/2015 12:41:19 Replay end rcvd                0           0

   MA: atm_ma       inited:0, flags:0x 0, circuits:0
   MA: hdlc_ma      inited:0, flags:0x 0, circuits:0
   MA: fr_ma        inited:0, flags:0x 0, circuits:0
   MA: ppp_ma       inited:0, flags:0x 0, circuits:0
   MA: cem_ma       inited:0, flags:0x 0, circuits:0
   MA: vif_ma       inited:0, flags:0x 0, circuits:0
   MA: pwhe_ma      inited:0, flags:0x 0, circuits:0
   MA: nve_mgr      inited:0, flags:0x 0, circuits:0
   MA: mstp         inited:0, flags:0x 0, circuits:0
   MA: span         inited:0, flags:0x 0, circuits:0
   MA: erp          inited:0, flags:0x 0, circuits:0
   MA: erp_test     inited:0, flags:0x 0, circuits:0
```

```
MA: mstp_test    inited:0, flags:0x 0, circuits:0
MA: evpn         inited:0, flags:0x 0, circuits:0
```

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information

show l2vpn forwarding

To display forwarding information from the layer2_fib manager, use the **show l2vpn forwarding** command in EXEC mode.

show l2vpn forwarding {**counter** | **debug** | **detail** | **hardware** | **interface** | **location** [*node-id*] | **private**}

Syntax Description

counter	Displays the cross-connect counters.
debug	Displays debug information.
detail	Displays detailed information from the layer2_fib manager.
hardware	Displays hardware-related layer2_fib manager information.
interface	Displays the match AC subinterface.
location *node-id*	Displays layer2_fib manager information for the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.
private	Output includes private information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following sample output is from the **show l2vpn forwarding** command:

```
Router# show l2vpn forwarding location 0/RP0/CPU0
Mon Oct 12 14:19:11.771 UTC
Segment 1                           Segment 2                           State
----------------------------------- ----------------------------------- ------
Te0/0/0/0.234                       ac Te0/0/0/26.234                   UP
Te0/0/0/0.233                       ac Te0/0/0/26.233                   UP
Te0/0/0/0.232                       ac Te0/0/0/26.232                   UP
Te0/0/0/0.231                       ac Te0/0/0/26.231                   UP
Te0/0/0/0.230                       ac Te0/0/0/26.230                   UP
```

The following sample output is from the **show l2vpn forwarding counter location** command:

```
Router# show l2vpn forwarding counter location 0/RP0/CPU0

Mon Oct 12 14:18:01.194 UTC
Legend: ST = State, DN = Down

Segment 1                         Segment 2                         ST Byte
                                                                       Switched
--------------------------------- --------------------------------- -- ---------
Te0/0/0/0.234                     ac Te0/0/0/26.234                 UP 15098997504
Te0/0/0/0.233                     ac Te0/0/0/26.233                 UP 15098997568
Te0/0/0/0.232                     ac Te0/0/0/26.232                 UP 15098997504
Te0/0/0/0.231                     ac Te0/0/0/26.231                 UP 15098997568
Te0/0/0/0.230                     ac Te0/0/0/26.230                 UP 15098997568
```

The following sample output is from the **show l2vpn forwarding summary location** command:

```
Router# show l2vpn forwarding summary location 0/RP0/CPU0
 Mon Oct 12 14:18:25.838 UTC
 To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Major version num:1, minor version num:0
Shared memory timestamp:0xa41120d180
Global configuration:
Number of forwarding xconnect entries:1873
  Up:1873  Down:0
  AC-PW(atom):0 AC-PW(l2tpv2):0 AC-PW(l2tpv3):0
  AC-PW(l2tpv3-ipv6):0
  AC-AC:1873  AC-BP:0 (PWHE AC-BP:0) AC-Unknown:0
  PW-BP:0  PW-Unknown:0
  PBB-BP:0  PBB-Unknown:0
  EVPN-BP:0  EVPN-Unknown:0
  VNI-BP:0 VNI-Unknown:0
  Monitor-Session-PW:0  Monitor-Session-Unknown:0
Number of xconnects down due to:
  AIB:0  L2VPN:0  L3FIB:0  VPDN:0
Number of xconnect updates dropped due to:
  Invalid XID: 0 VPWS PW, 0 VPLS PW, 0 Virtual-AC, 0 PBB,
 0 EVPN
 0 VNI
Exceeded max allowed: 0 VPLS PW, 0 Bundle-AC
Number of p2p xconnects: 1873
Number of bridge-port xconnects: 0
Number of nexthops:0
Number of bridge-domains: 0
  0 with routed interface
  0 with PBB-EVPN enabled
  0 with EVPN enabled
  0 with p2mp enabled
Number of bridge-domain updates dropped: 0
Number of total macs: 0
  0 Static macs
  0 Routed macs
  0 BMAC
  0 Source BMAC
  0 Locally learned macs
  0 Remotely learned macs
Number of total P2MP Ptree entries: 0
Number of PWHE Main-port entries: 0
Number of EVPN Multicast Replication lists: 0 (0 default)
```

The following sample output is from the **show l2vpn forwarding detail location** command:

```
Router# show l2vpn forwarding detail location 0/RP0/CPU0

Mon Oct 12 14:18:47.187 UTC
Local interface: TenGigE0/0/0/0.234, Xconnect id: 0x1, Status: up
  Segment 1
    AC, TenGigE0/0/0/0.234, status: Bound
    Statistics:
      packets: received 238878391, sent 313445
      bytes: received 15288217024, sent 20060480
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0
  Segment 2
    AC, TenGigE0/0/0/26.234, status: Bound

Local interface: TenGigE0/0/0/0.233, Xconnect id: 0x2, Status: up
  Segment 1
    AC, TenGigE0/0/0/0.233, status: Bound
    Statistics:
      packets: received 238878392, sent 313616
      bytes: received 15288217088, sent 20071424
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0
  Segment 2
    AC, TenGigE0/0/0/26.233, status: Bound

Local interface: TenGigE0/0/0/0.232, Xconnect id: 0x3, Status: up
 Segment 1
    AC, TenGigE0/0/0/0.232, status: Bound
    Statistics:
      packets: received 238878391, sent 313476
      bytes: received 15288217024, sent 20062464
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0
  Segment 2
    AC, TenGigE0/0/0/26.232, status: Bound
```

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information
show l2vpn database, on page 45	Displays L2VPN database
show l2vpn forwarding message counters, on page 51	Displays l2vpn forwarding message counters information.

show l2vpn forwarding message counters

To display L2VPN forwarding messages exchanged with L2FIB Collaborators, use the **show l2vpn forwarding message counters** command in EXEC mode.

show l2vpn forwarding message counters {**hardware** | **location** *node-id*}

Syntax Description

hardware	Displays message counter information from hardware.
location *node-id*	Displays message counter information for the specified location.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Even when xSTP (extended spanning tree protocol) operates in the PVRST mode, the output of the show or debug commands flag prefix is displayed as MSTP or MSTi, instead of PVRST.

Task ID

Task ID	Operation
l2vpn	read

The following examples shows the output from the **show l2vpn forwarding message counters location** command:

```
Router# show l2vpn forwarding message counters location 0/RP0/CPU0
Mon Oct 12 14:19:41.768 UTC
Messages exchanged with L2FIB Collaborators:
-------------------------------------------------------------------------------
     Message                                          Count       Info1        Info2
    Time
     =======                                          =====       =====        =====
    ====
     l2vpn provision messages received:                7496       0x800001c    0x0
    Oct 12 13:09:38.477
     l2vpn unprovision messages received:              0          0x0          0x0
    -
     l2vpn bridge provision messages received:         0          0x0          0x0
    -
     l2vpn bridge unprovision messages received:       0          0x0          0x0
    -
     l2vpn bridge main port update messages received:  0          0x0          0x0
    -
     bdxc bridge main port update messages received:   0          0x0          0x0
    -
     l2vpn bridge main port update w/ action=MSTI_DELETE 0        0x0          0x0
    -
     l2vpn bridge main port update ACK sent:           0          0x0          0x0
```

```
-
 bdxc bridge main port update ACK sent:              0          0x0          0x0
-
 l2vpn reception of ACK relay msg received:          0          0x0          0x0
-
 l2vpn bridge port provision messages received:      0          0x0          0x0
-
 l2vpn bridge port unprovision messages received:    0          0x0          0x0
-
 l2vpn shg provision messages received:              0          0x0          0x0
-
 l2vpn shg unprovision messages received:            0          0x0          0x0
-
 l2vpn static mac provision messages received:       0          0x0          0x0
-
 l2vpn static mac unprovision messages received:     0          0x0          0x0
-
 l2vpn static mac flush messages received:           0          0x0          0x0
-
 l2vpn dynamic mac local learning messages received: 0          0x0          0x0
-
 l2vpn dynamic mac local learning dropped queue len: 0          0x0          0x0
-
 l2vpn dynamic mac local learning dropped cache:     0          0x0          0x0
-
 l2vpn dynamic mac local learning dropped multicast: 0          0x0          0x0
-
 l2vpn dynamic mac bcast send failed:                0          0x0          0x0
-
 l2vpn dynamic mac remote learning messages received 0          0x0          0x0
-
 l2vpn dynamic mac refresh messages received:        0          0x0          0x0
-
 l2vpn dynamic mac delete/create messages received:  0          0x0          0x0
-
 l2vpn dynamic mac no-xid dropped:                   0          0x0          0x0
-
 l2vpn dynamic local mac unprovision messages:       0          0x0          0x0
-
 l2vpn dynamic remote mac unprovision messages:      0          0x0          0x0
-
 l2vpn dynamic local mac aged out messages sent:     0          0x0          0x0
-
 l2vpn dynamic mac limit message received:           0          0x0          0x0
-
 l2vpn dynamic mac delete notification:              0          0x0          0x0
-
 l2vpn mac move counter:                             0          0x0          0x0
-
 l2vpn qid mac remote:                               0          0x0          0x0
-
 l2vpn qid mac remote evpn:                          0          0x0          0x0
-
 l2vpn qid mac refresh:                              0          0x0          0x0
-
 l2vpn qid mac learning:                             0          0x0          0x0
-
 AIB update messages received:                       7494       0x8007502    0x8000150
Oct 12 12:49:44.112
 AIB delete messages received:                      0          0x0          0x0
-
 FIB nhop registration messages sent:               0          0x0          0x0
-
 FIB nhop unregistration messages sent:             0          0x0          0x0
```

```
-
 FIB ecd ldi update messages received:               0          0x0          0x0
-
 FIB invalid NHOP prov messages received:            0          0x0          0x0
-
 l2vpn hw learn MAC update messages received:        0          0x0          0x0
-
 l2vpn hw learn MAC BD limit set messages received:  0          0x0          0x0
-
 l2vpn hw learn MAC BD limit clr messages received:  0          0x0          0x0
-
 l2vpn hw learn MAC BP limit set messages received:  0          0x0          0x0
-
 l2vpn hw learn MAC BP limit clr messages received:  0          0x0          0x0
-
 l2vpn backbone source mac provision msg received:   1          0x0          0x0
Oct 12 12:41:19.807
 l2vpn backbone source mac unprovision msg received: 0          0x0          0x0
-
 l2vpn bridge port MAC flush msg received:           0          0x0          0x0
-
 bdxc ISSU drop msg received:                        0          0x0          0x0
-
 l2vpn ISSU drop msg received:                       0          0x0          0x0
-
 l2vpn BD MAC Flush messages received:               0          0x0          0x0
-
 l2vpn TCN messages received:                        0          0x0          0x0
-
 bdxc G8032 TCN messages transmitted:                0          0x0          0x0
-
 l2fib PD failure count:                             0          0x0          0x0
-
 bdxc DHCP binding provision msg received:           0          0x0          0x0
-
 bdxc DHCP binding unprovision msg received:         0          0x0          0x0
-
 bdxc DHCP configuration msg received:               0          0x0          0x0
-
 platform DAI violation msg received:                0          0x0          0x0
-
 platform IPSG violation msg received:               0          0x0          0x0
-
 platform MAC Secure violation msg received:         0          0x0          0x0
-
 l2vpn g8032 ring provision msg received:            0          0x0          0x0
-
 l2vpn g8032 ring unprovision msg received:          0          0x0          0x0
-
 l2vpn g8032 ring inst provision msg received:       0          0x0          0x0
-
 l2vpn g8032 ring inst unprovision msg received:     0          0x0          0x0
-
 bdxc VPDN L2TPv2 provision msg received:            0          0x0          0x0
-
 bdxc VPDN L2TPv2 unprovision msg received:          0          0x0          0x0
-
 bdxc VPDN L2TPv2 invalid msg received:              0          0x0          0x0
-
 bdxc P2MP PTREE provision msg received:             0          0x0          0x0
-
 bdxc P2MP PTREE unprovision msg received:           0          0x0          0x0
-
 bdxc P2MP PTREE provision msg dropped:              0          0x0          0x0
```

```
-
 bdxc P2MP PTREE unprovision msg dropped:            0          0x0          0x0
-
 l2vpn reception of protection ack msg received:     0          0x0          0x0
-
 l2vpn GLOBAL messages received:                     1          0x0          0x0
Oct 12 12:41:19.807
 l2vpn BD Flush request messages to l2vpn:           0          0x0          0x0
-
 l2vpn evpn mcast provision msg received:            0          0x0          0x0
-
 l2vpn evpn mcast unprovision msg received:          0          0x0          0x0
-
 l2vpn evpn mcast invalid msg received:              0          0x0          0x0
-
 l2vpn evpn mcast unprovision all msg received:      0          0x0          0x0
-
 l2vpn evpn main port provision msg received:        0          0x0          0x0
-
 l2vpn evpn main port unprovision msg received:      0          0x0          0x0
-
 l2vpn evpn main port invalid msg received:          0          0x0          0x0
-
 l2vpn MVRP request:                                 0          0x0          0x0
-
 l2vpn pwgroup status update msg received:           0          0x0          0x0
-
```

The following examples shows the output from the **show l2vpn forwarding message counters hardware location** command:

```
Router# show l2vpn forwarding message counters hardware location 0/$
Mon Oct 12 14:19:59.017 UTC

                          Event Statistics Summary
-----------------------------------------------------------------------
             Create      Modify        Bind       Unbind      Delete
 LOCXC AC      7492        3748        7496            4           0
 VPWS  AC         0           0           0            0           0
 VPLS  AC         0           0           0            0           0
 L2TP  AC         0           0           0            0           0
 VPWS  PW         0           0           0            0           0
 VPLS  PW         0           0           0            0           0
 BRIDGE           0           0           0            0           0
 BRIDGEPORT       0           0           0            0           0
 MAC              0           0           0            0           0
 PBB              0           0           0            0           0
 DHCP             0           0           0            0           0
 L2TP             0           0           0            0           0
 L2TP SESSION     0           0           0            0           0


                       Performance Statistics Summary
-----------------------------------------------------------------------
                  Create     Modify     Delete       Bind     Unbind
 LOCXC AC      000.032 s  000.790 s     < 1 ms  000.810 s  000.003 s
 VPWS  AC         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 VPLS  AC         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 L2TP  AC         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 VPWS  PW         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 VPLS  PW         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 BRIDGE           < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 BRIDGEPORT       < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 MAC              < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
```

```
PBB              < 1 ms      < 1 ms      < 1 ms      < 1 ms      < 1 ms
DHCP             < 1 ms      < 1 ms      < 1 ms      < 1 ms      < 1 ms
L2TP             < 1 ms      < 1 ms      < 1 ms      < 1 ms      < 1 ms
L2TP SESSION     < 1 ms      < 1 ms      < 1 ms      < 1 ms      < 1 ms
```

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information
show l2vpn database, on page 45	Displays L2VPN database
show l2vpn forwarding, on page 48	Displays forwarding information from the layer2_fib manager on the line card.

show l2vpn index

To display statistics about the index manager, use the **show l2vpn index** command in EXEC mode.

show l2vpn index [{**location** | **private**}]**private**

Syntax Description

location	(Optional) Displays index manager statistics for the specified location.
private	(Optional) Detailed information about all indexes allocated for each pool.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read

Examples

This example shows the sample output of the **show l2vpn index** command:

```
Router# show l2vpn index
 Mon Oct 12 14:20:20.218 UTC
 Pool id: 0x0, App: AC
   Max number of ID mgr instances: 1
   ID mgr instances in use: 1
   Pool size: 32513
   zombied IDs: 0
   allocated IDs: 3745

 Pool id: 0xfff80002, App: BD
   Max number of ID mgr instances: 1
   ID mgr instances in use: 1
   Pool size: 8192
   zombied IDs: 0
   allocated IDs: 0

 Pool id: 0xfff80003, App: MP2MP
   Max number of ID mgr instances: 1
   ID mgr instances in use: 1
   Pool size: 65535
   zombied IDs: 0
```

```
  allocated IDs: 0

Pool id: 0xfff80004, App: RD
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 65536
  zombied IDs: 0
  allocated IDs: 0

Pool id: 0xfff80005, App: IFLIST
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 65535
  zombied IDs: 0
  allocated IDs: 1

Pool id: 0xfff80006, App: ATOM
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 131071
  zombied IDs: 0
  allocated IDs: 0

Pool id: 0xfff80007, App: PWGroup
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 65535
  zombied IDs: 0
  allocated IDs: 1

Pool id: 0xfffd0000, App: Global
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 16383
  zombied IDs: 0
  allocated IDs: 2
```

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information
show l2vpn database, on page 45	Displays L2VPN database
show l2vpn forwarding, on page 48	Displays forwarding information from the layer2_fib manager on the line card.

show l2vpn resource

To display the memory state in the L2VPN process, use the **show l2vpn resource** command in EXEC mode.

show l2vpn resource

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows sample output for the **show l2vpn resource** command:

```
Router# show l2vpn resource
Mon Oct 12 14:21:54.670 UTC
Memory: Normal
```

This table describes the significant fields shown in the display.

Table 3: show l2vpn resource Command Field Descriptions

Field	Description
Memory	Displays memory status.

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information
show l2vpn index, on page 56	Displays statistics about the index manager.

show l2vpn trace

To display trace data for L2VPN, use the **show l2vpn trace** command in EXEC mode.

show l2vpn trace [{**checker** | **file** | **hexdump** | **last** | **location** | **reverse** | **stats** | **tailf** | **unique** | **usec** | **verbose** | **wide** | **wrapping**}]

Syntax Description

checker	Displays trace data for the L2VPN Uberverifier.
file	Displays trace data for the specified file.
hexdump	Display traces data in hexadecimal format.
last	Display last <n> entries
location	Displays trace data for the specified location.
reverse	Display latest traces first
stats	Display trace statistics
tailf	Display new traces as they are added
unique	Display unique entries with counts
usec	Display usec details with timestamp
verbose	Display internal debugging information
wide	Display trace data excluding buffer name, node name, tid
wrapping	Display wrapping entries

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

This example displays output for the **show l2vpn trace** command:

```
Router# show l2vpn trace
Mon Oct 12 14:22:09.082 UTC
188 unique entries (2596 possible, 0 filtered)
Oct 12 12:37:44.197 l2vpn/policy 0/RP0/CPU0 1# t4349 POLICY:320: l2vpn_policy_reg_agent
started - route_policy_supported=False, forward_class_supported=False
Oct 12 12:39:21.870 l2vpn/fwd-pd 0/RP0/CPU0 1# t5664 FWD_PD:731:
Oct 12 12:39:21.883 l2vpn/fwd-err 0/RP0/CPU0 1# t5664 FWD_ERR|ERR:76: Major version mis-match,
 SHM: 0x0 Expected: 0x1
Oct 12 12:39:21.883 l2vpn/fwd-err 0/RP0/CPU0 1# t5664 FWD_ERR|ERR:87: Magic number mis-match,
 SHM: 0x0 Expected: 0xa7b6c3d8
Oct 12 12:39:21.884 l2vpn/err 0/RP0/CPU0 1# t5664 FWD_ERR|ERR:76: Major version mis-match,
 SHM: 0x0 Expected: 0x1
Oct 12 12:39:21.884 l2vpn/err 0/RP0/CPU0 1# t5664 FWD_ERR|ERR:87: Magic number mis-match,
SHM: 0x0 Expected: 0xa7b6c3d8
Oct 12 12:39:21.890 l2vpn/fwd-detail 0/RP0/CPU0 1# t5664 FWD_DETAIL:263: PWGROUP Table init
 succeeded
Oct 12 12:39:21.890 l2vpn/fwd-detail 0/RP0/CPU0 2# t5664 FWD_DETAIL:416: l2tp session table
 rebuilt
Oct 12 12:39:21.903 l2vpn/fwd-common 0/RP0/CPU0 1# t5664 FWD_COMMON:39: L2FIB_OBJ_TRACE:
trace_buf=0x7d48e0
Oct 12 12:39:25.613 l2vpn/issu 0/RP0/CPU0 1# t5664 ISSU:790: ISSU - iMDR init called;
'infra/imdr' detected the 'informational' condition 'the service is not supported in the
node'
Oct 12 12:39:25.613 l2vpn/issu 0/RP0/CPU0 1# t5664 ISSU:430: ISSU - attempt to start
COLLABORATOR wait timer while not in ISSU mode
Oct 12 12:39:25.638 l2vpn/fwd-common 0/RP0/CPU0 1# t5664 FWD_COMMON:4241: show edm thread
initialized
Oct 12 12:39:25.781 l2vpn/fwd-mac 0/RP0/CPU0 1# t5664 FWD_MAC|ERR:783: Mac aging init
Oct 12 12:39:25.781 l2vpn/fwd-mac 0/RP0/CPU0 2# t5664 FWD_MAC:1954: l2vpn_gsp_cons_init
returned Success
Oct 12 12:39:25.781 l2vpn/err 0/RP0/CPU0 1# t5664 FWD_MAC|ERR:783: Mac aging init
Oct 12 12:39:25.782 l2vpn/fwd-aib 0/RP0/CPU0 4# t5664 FWD_AIB:446: aib connection opened
successfully
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 2# t5664 FWD_MAC:2004: Client successfully
joined gsp group
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 1# t5664 FWD_MAC:781: Initializing the txlist
 IPC thread
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 1# t5664 FWD_MAC:3195: gsp_optimal_msg_size =
 31264 (real: True)
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 1# t5664 FWD_MAC:626: Entering mac aging timer
 init
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 1# t7519 FWD_MAC:725: Entering event loop for
 mac txlist thread
Oct 12 12:39:25.797 l2vpn/fwd-mac 0/RP0/CPU0 1# t4222 FWD_MAC:2221: learning_client_colocated
 0, is_client_netio 1
```

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information
show l2vpn index, on page 56	Displays statistics about the index manager.

Command	Description
show l2vpn resource, on page 58	Displays the memory state in the L2VPN process.

show l2vpn xconnect

To display brief information on configured cross-connects, use the **show l2vpn xconnect** command in EXEC mode.

show l2vpn xconnect [{**brief** | **detail***encapsulation* | **group** | **groups** | **interface** | **location** | **neighbor** | **standby** | **state** | **summary** | **type locally-switched**}]

Syntax Description

brief	(Optional) Displays encapsulation brief information.
detail	(Optional) Displays detailed information.
encapsulation	(Optional) Filters on encapsulation type.
group	(Optional) Displays all cross-connects in a specified group.
groups	(Optional) Displays all groups information.
interface	(Optional) Filters on interface and subinterface.
location	(Optional) Displays location specific information.
neighbor	(Optional) Filters on neighbor.
private	(Optional) Displays private information.
standby	(Optional) Displays standby node specific information.
state	(Optional) Filters the following xconnect state types: • up • down
summary	(Optional) Displays AC information from the AC Manager database.
type	(Optional) Filters the locally switched xconnect type.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.4.1	

Usage Guidelines

If a specific cross-connect is specified in the command then only that cross-connect will be displayed; otherwise, all cross-connects are displayed.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows sample output for the **show l2vpn xconnect** command:

```
Router# show l2vpn xconnect
Mon Oct 12 14:22:20.566 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
XConnect                    Segment 1                       Segment 2
Group      Name       ST    Description             ST      Description             ST
------------------------    ------------------------------  ------------------------------
XC         XC         UP    BE1                     UP      BE2                     UP
-----------------------------------------------------------------------------------------
XCON31     XCON1_P2P1 UP    Te0/0/0/0.1             UP      Te0/0/0/26.1            UP
-----------------------------------------------------------------------------------------
XCON32     XCON1_P2P2 UP    Te0/0/0/0.2             UP      Te0/0/0/26.2            UP
-----------------------------------------------------------------------------------------
XCON33     XCON1_P2P3 UP    Te0/0/0/0.3             UP      Te0/0/0/26.3            UP
-----------------------------------------------------------------------------------------
XCON34     XCON1_P2P4 UP    Te0/0/0/0.4             UP      Te0/0/0/26.4            UP
-----------------------------------------------------------------------------------------
XCON35     XCON1_P2P5 UP    Te0/0/0/0.5             UP      Te0/0/0/26.5            UP
-----------------------------------------------------------------------------------------
XCON36     XCON1_P2P6 UP    Te0/0/0/0.6             UP      Te0/0/0/26.6            UP
-----------------------------------------------------------------------------------------
XCON37     XCON1_P2P7 UP    Te0/0/0/0.7             UP      Te0/0/0/26.7            UP
-----------------------------------------------------------------------------------------
XCON38     XCON1_P2P8 UP    Te0/0/0/0.8             UP      Te0/0/0/26.8            UP
-----------------------------------------------------------------------------------------
```

This example shows the output of the **show run l2vpn** command :

```
Router# show run l2vpn

Mon Oct 12 14:23:24.723 UTC
l2vpn
 xconnect group XC
  p2p XC
   interface Bundle-Ether1
   interface Bundle-Ether2
  !
 !
 xconnect group XCON31
  p2p XCON1_P2P1
   interface TenGigE0/0/0/0.1
   interface TenGigE0/0/0/26.1
  !
 !
 xconnect group XCON32
  p2p XCON1_P2P2
   interface TenGigE0/0/0/0.2
   interface TenGigE0/0/0/26.2
  !
 !
 xconnect group XCON33
  p2p XCON1_P2P3
```

```
interface TenGigE0/0/0/0.3
interface TenGigE0/0/0/26.3
```

This table describes the significant fields shown in the display.

Table 4: show l2vpn xconnect Command Field Descriptions

Field	Description
XConnect Group	Displays a list of all configured cross-connect groups.
Group	Displays the cross-connect group number.
Name	Displays the cross-connect group name.
Description	Displays the cross-connect group description. If no description is configured, the interface type is displayed.
ST	State of the cross-connect group: up (UP) or down (DN).

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information
show l2vpn database, on page 45	Displays L2VPN database
show l2vpn pw-class, on page 65	Displays L2VPN pseudowire class information.

show l2vpn pw-class

To display L2VPN pseudowire class information, use the **show l2vpn pw-class** command in EXEC mode.

show l2vpn pw-class [{**detail** | **location** | **name** *class name* | **standby**}]

Syntax Description

detail	(Optional) Displays detailed information.
location	(Optional) Displays location specific information.
name *class-name*	(Optional) Displays information about a specific pseudowire class name.
standby	(Optional) Displays standby node specific information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows sample output for the **show l2vpn pw-class** command:

```
Router# show l2vpn pw-class

Name                         Encapsulation     Protocol
-------------------------    ----------        ----------
mplsclass_75                 MPLS              LDP
l2tp-dynamic                 L2TPv3            L2TPv3
```

This example shows sample output for the **show l2vpn pw-class detail** command:

```
Router# show l2vpn pw-class detail
    Encapsulation MPLS, protocol LDP
    Transport mode not set, control word unset (default)
    Sequencing not set
    Static tag rewrite not set
    PW Backup disable delay: 0 sec
    MAC withdraw message is sent over PW: no
    IPv4 source address 10.0.0.1
```

This table describes the significant fields shown in the display.

Table 5: show l2vpn pw-class Command Field Descriptions

Field	Description
Name	Displays the name of the pseudowire class.
Encapsulation	Displays the encapsulation type.
Protocol	Displays the protocol type.

Related Commands

Command	Description
l2vpn, on page 26	Enters L2VPN configuration mode.
p2p, on page 32	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 33	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 37	Displays L2VPN information
show l2vpn database, on page 45	Displays L2VPN database

storm-control

To enable storm control on an access circuit (AC) under a VPLS bridge, use the **storm-control** command in l2vpn bridge group bridge-domain access circuit configuration mode. To disable storm control, use the **no** form of this command.

storm-control {**broadcast** | **multicast** | **unknown-unicast**} {**pps** *pps-value* | **kbps** *kbps-value*}
no storm-control {**broadcast** | **multicast** | **unknown-unicast**} {**pps** *pps-value* | **kbps** *kbps-value*}

Syntax Description

broadcast	Configures storm control for broadcast traffic.
multicast	Configures storm control for multicast traffic.
unknown-unicast	Configures storm control for unknown unicast traffic. • Storm control does not apply to bridge protocol data unit (BPDU) packets. All BPDU packets are processed as if traffic storm control is not configured. • Storm control does not apply to internal communication and control packets, route updates, SNMP management traffic, Telnet sessions, or any other packets addressed to the router.
pps *pps-value*	Configures the packets-per-second (pps) storm control threshold for the specified traffic type. Valid values range from 1 to 160000.
kbps *kbps-value*	Configures the storm control in kilo bits per second (kbps). The range is from 64 to 1280000.

Command Default

Storm control is disabled by default.

Command Modes

l2vpn bridge group bridge-domain access circuit configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

- The storm control configuration is supported only on one sub-interface under a main interface, though the system allows you to configure storm control on more than one sub-interface. However, only the first storm control configuration under a main interface takes effect, though the running configuration shows all the storm control configurations that are committed. After reload, any of the storm control configurations may take effect irrespective of the order of configuration.
- Starting from 7.8.1, you can enable per subinterface configuration support for storm control by using the **hw-module storm-control-combine-policer-bw enable** command.
- System supports storm control per-EFP.
- If storm control is applied on one bridge port, you cannot apply storm control on another bridge port or sub-interface under the same main-port. On configuring, system pop-ups an error, but needs to be manually unconfigured.

- System does not support storm control on pseudowire bridge-ports.
- Storm control counters are not supported
- Only kbps rate is supported by hardware. Though the pps configuration is allowed, it is converted to kbps. The pps rate is calculated as 1 pps = 8 kbps.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example enables two storm control thresholds on an access circuit:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group csco
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet0/1/0/0.100
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# storm-control broadcast kbps 4500
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# commit
```

xconnect group

To configure cross-connect groups, use the **xconnect group** command in L2VPN configuration mode. To return to the default behavior, use the **no** form of this command.

xconnect group *group-name*
no xconnect group *group-name*

Syntax Description

group-name	Configures a cross-connect group name using a free-format 32-character string.

Command Default

None

Command Modes

L2VPN configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Note You can configure up to a maximum of 16K cross-connects per box.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to group all cross-connects for XCON1:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface gigabitethernet0/1/0/0.1
Router(config-l2vpn-xc-p2p)# neighbor 10.165.100.151 pw-id 100
Router(config-l2vpn-xc-p2p-pw)# mpls static label local 50 remote 40
Router(config-l2vpn-xc-p2p-pw)# commit
```

Related Commands

Command	Description
interface (p2p), on page 18	Configures an attachment circuit.
l2vpn, on page 26	Enters L2VPN configuration mode.
show l2vpn, on page 37	Displays L2VPN information

Command	Description
show l2vpn xconnect, on page 62	Displays brief information on configured cross-connects.

L2VPN Autodiscovery and Signaling Commands

This section describes the commands used to configure L2VPN Autodiscovery and Signaling feature.

For detailed information about concepts and configuration, see the *Configure L2VPN Autodiscovery and Signaling* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5000 Series Routers*.

autodiscovery bgp

To enable BGP autodiscovery for the L2VPN service, use the **autodiscovery bgp** command in the **vfi** configuration mode for VPLS and **mp2mp** configuration mode for VPWS. To disable BGP autodiscovery, use the **no** form of this command.

autodiscovery bgp

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

VFI configuration mode and mp2mp configuration mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable bgp autodiscovery for VPLS:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group EGroup
Router(config-l2vpn-bg)# bridge-domain eastdomain
Router(config-l2vpn-bg-bd)# vfi eastvfi
Router(config-l2vpn-bg-bd-vfi)# autodiscovery bgp
```

The following example shows how to enable bgp autodiscovery for VPWS:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group WGroup
Router(config-l2vpn-xc)# mp2mp westside
Router(config-l2vpn-xc-mp2mp)# vpn-id 100
Router(config-l2vpn-xc-mp2mp)# l2-encapsulation vlan
Router(config-l2vpn-xc-mp2mp)# autodiscovery bgp
```

signaling-protocol

To enable the preferred signaling protocol for the VFI, use the **signaling-protocol** command in the BGP autodiscovery mode. To return to the default value, use the **no** form of this command.

signaling-protocol {**bgp** | **ldp**}

Syntax Description

bgp	Enables BGP protocol signaling.
ldp	Enables LDP protocol signaling.

Command Default

LDP signaling is enabled.

Command Modes

BGP autodiscovery configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to enable the preferred signaling-protocol for VPLS:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group EGroup
Router(config-l2vpn-bg)# bridge-domain eastdomain
Router(config-l2vpn-bg-bd)# vfi eastvfi
Router(config-l2vpn-bg-bd-vfi)# autodiscovery bgp
Router(config-l2vpn-bg-bd-vfi-ad)#route-target 100:20
Router(config-l2vpn-bg-bd-vfi-ad)#signaling-protocol bgp
```

This example shows how to enable the preferred signaling-protocol for VPWS:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group WGroup
Router(config-l2vpn-xc)# mp2mp westside
Router(config-l2vpn-xc-mp2mp)# vpn-id 100
Router(config-l2vpn-xc-mp2mp)# l2-encapsulation vlan
Router(config-l2vpn-xc-mp2mp)# autodiscovery bgp
Router(config-l2vpn-xc-mp2mp-ad)# route-target 2.2.2.2:100
Router(config-l2vpn-xc-mp2mp-ad)# signaling-protocol ldp
```

Multiple Spanning Tree Protocol Commands

This section describes the commands used to configure Multiple Spanning Tree Protocol (MSTP) feature.

For detailed information about concepts and configuration, see the *Configure Multiple Spanning Tree Protocol* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5000 Series Routers*.

instance (MSTP)

In order to configure the multiple spanning tree instance (MSTI), use the **instance** command in MSTP configuration submode.

instance *id*

Syntax Description

id	MSTI ID. Range is 0 to 4094.

Command Default

None

Command Modes

MSTP configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

Note An instance ID of 0 represents the Common Internal Spanning Tree (CIST) for the region.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MSTI configuration submode:

```
RP/0/RP0/CPU0:router(config-mstp)# instance 101
RP/0/RP0/CPU0:router(config-mstp-inst)#
```

interface (MSTP)

To enter the MSTP interface configuration submode, use the **interface** command in MSTP configuration submode.

interface *interface-type interface-path-id*

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

None

Command Modes

MSTP configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

A given port may only be enabled with one of MSTP, MSTAG, REPAG, PVSTAG, or PVRSTAG.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MSTP interface configuration submode:

```
Router(config-mstp)# interface GigabitEthernet 0/0/0/7
```

name (MSTP)

To set the name of the MSTP region, use the **name** command in MSTP configuration submode.

name *name*

Syntax Description

name	String of a maximum of 32 characters conforming to the definition of SnmpAdminString in RFC 2271.

Command Default

The MAC address of the switch, formatted as a text string using the hexadecimal representation specified in IEEE Std 802.

Command Modes

MSTP configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the name of the MSTP region to m1:

```
RP/0/RP0/CPU0:router(config-mstp)# name m1
```

portfast

To enable PortFast feature on the port and enable BPDU guard, use the **portfast** command in MSTP interface configuration submode.

portfast [**bpduguard**]

Syntax Description

This command has no keywords or arguments.

Command Default

PortFast is disabled.

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

This command enables the portfast feature (also known as edge port). When this is enabled, MSTP treats the port as an edge port, i.e., it keeps it in forwarding state and does not generate topology changes if the port goes down or comes up. It is not expected to receive MSTP BPDUs on an edge port. BPDU guard is a Cisco extension that causes the interface to be shut down using error-disable if an MSTP BPDU is received.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enable PortFast and BPDU guard on the port:

```
Router(config-mstp-if)# portfast
Router(config-mstp-if)# portfast bpduguard
```

show spanning-tree mst

To display the multiple spanning tree protocol status information, use the **show spanning-tree mst** command in EXEC mode.

show spanning-tree mst *protocol-instance-identifier* [**instance** *instance-id*] [{**blocked-ports** | **brief**}]

Syntax Description

protocol-instance-identifier	String of a maximum of 25 characters that identifies the protocol instance.
instance *instance-id*	Forward interface in rack/slot/instance/port format.
brief	Displays a summary of MST information only.
blocked-ports	Displays MST information for blocked ports only.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mst** command, which produces an overview of the spanning tree protocol state:

```
RP/0/RP0/CPU0:router# show spanning-tree mst a instance 0
Operating in Provider Bridge mode
MSTI 0 (CIST):

  VLANS Mapped: 1-100, 500-1000, 1017

  Root ID    Priority    4097
             Address     0004.9b78.0800
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec


  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     0004.9b78.0800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Interface                Port ID                     Designated               Port ID
Name                     Prio.Nbr Cost   Role State  Cost Bridge ID           Prio.Nbr
-----------------------  -------- ------ ---------  ------------------------ --------
GigabitEthernet0/1/2/1   128.65   20000  DSGN FWD    0    4097 0004.9b78.0800 128.65
GigabitEthernet0/1/2/2   128.66   20000  DSGN FWD    0    4097 0004.9b78.0800 128.66
...
```

The following example shows the output from the **show spanning-tree mst** command when the **brief** and **blocked-ports** keywords are used:

```
RP/0/RP0/CPU0:router# show spanning-tree mst a brief
MSTI 0 (CIST):
  VLAN IDs: 1-100, 500-1000, 1017
  This is the Root Bridge
MSTI 1:
  VLAN IDS: 101-499
  Root Port GigabitEthernet0/1/2/2  , Root Bridge ID 0002.9b78.0812
...
RP/0/RP0/CPU0:router# show spanning-tree mst blocked-ports
MSTI 0 (CIST):

Interface                Port ID                     Designated               Port ID
Name                     Prio.Nbr Cost   Role State  Cost Bridge ID           Prio.Nbr
-----------------------  -------- ------ ---------  ------------------------ --------
GigabitEthernet0/0/4/4      128.196  200000 ALT  BLK    0    4097 0004.9b78.0800 128.195
...
```

spanning-tree mst

To enter the MSTP configuration submode, use the **spanning-tree mst** command in global configuration mode.

spanning-tree mst *protocol-instance-identifier*

Syntax Description

protocol-instance-identifier	String of a maximum of 25 characters that identifies the protocol instance.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

Note In MSTP configuration, only one protocol instance can be configured at a time.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MSTP configuration submode:

```
Router(config)# spanning-tree mst m0
```

vlan-ids (MSTP)

To associate a set of VLAN IDs with the current MSTI, use the **vlan-ids** command in MSTI configuration submode.

vlan-ids *vlan-range-list*

Syntax Description

vlan-range-list	A comma-separated list of VLAN ranges in the form a-b, c, d, e-f, g etc. Upto 3 ranges can be specified.

Command Default

None

Command Modes

MSTI configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to use the vlan-id command:

```
RP/0/RP0/CPU0:router(config-mstp-inst)# vlan-ids 2-1005
```