VPN and Ethernet Services Command Reference for Cisco 8000 Series Routers

First Published: 2021-02-01

Last Modified: 2024-03-14

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

CHAPTER 1

CHAPTER 2

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
March 2024	Republished with documentation updates for Release 24.1.1 features.
December 2023	Republished with documentation updates for Release 7.11.1 features.
October 2021	Republished with documentation updates for Release 7.3.2 features.
May 2021	Republished with documentation updates for Release 7.3.15 features.
February 2021	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.

EVPN Commands

This section describes the commands used to configure Ethernet VPN (EVPN) services for Layer 2 VPNs.

advertise-mac

To advertise local MAC to the peers, use **advertise-mac** command in the EVPN configuration mode. The local MAC is advertised to the peer in control plane using BGP.

advertise-mac

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EVPN

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

The following example shows how to advertise local MAC.

```
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether 1
Router(config-evpn-ac)# exit
Router(config-evpn)# evi 2001
Router(config-evpn-instance)# advertise-mac
Router(config-evpn-instance-mac)# commit
```

core-isolation-group

To configure EVPN core isolation group after the core interfaces fail, use the **core-isolation-group** command in the EVPN Timers configuration mode.

core-isolation-group *group-id*

Syntax Description

group-id	Specifies the core isolation group ID. The range is from 1 to 4294967295.

Command Default

None.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

This example shows how to configure the EVPN core isolation group.

```
Router# configure
Router(config-evpn)# interface bundle-Ether 43001
Router(config-evpn-ac)# core-isolation-group 43001
Router(config-evpn-ac)# commit
```

ethernet-segment

To enter the EVPN interface ethernet segment configuration mode, use the **ethernet-segment** command in the EVPN interface configuration mode. To disable the Ethernet segment configuration, use the **no** form of this command.

ethernet-segment [{ **backbone-source-mac** | **identifier** | **load-balancing-mode** | **service-carving** }]
no ethernet-segment [{ **backbone-source-mac** | **identifier** | **load-balancing-mode** | **service-carving** }]

Syntax Description

backbone-source-mac	Specifies Backbone Source MAC.
identifier	Specifies Ethernet Segment Identifier.
load-balancing-mode	Specifies load balancing mode.
service-carving	Specifies service carving.

Command Default

None.

Command Modes

EVPN interface configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to enter the EVPN interface ethernet segment configuration mode:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)#
```

etree rt-leaf

To enable EVPN instance as EVPN E-Tree leaf site using BGP Route Target (RT) import and export policies, use the **etree rt-leaf** command in the EVPN EVI configuration submode.

etree rt-leaf

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

EVI configuration submode

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to designate EVPN instance as EVPN E-Tree Route-Target leaf site.

```
Router(config)# evpn
Router(config-evpn)# evi 15
Router(config-evpn-instance)# etree
Router(config-evpn-instance-etree)# rt-leaf
```

evi

To enter the EVPN EVI configuration mode and configure BGP settings for a bridge domain or EVI, use the **evi** command in the EVPN configuration mode.

evi *evi-id*

Syntax Description

evi-id	Specifies the Ethernet VPN ID to set. The range is from 1 to 65534.

Command Default

None.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

Use this command to configure static BGP route distinguisher or BGP route target for an EVI.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enter the EVPN EVI configuration mode:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 2
```

evpn

To enter EVPN configuration mode, use the **evpn** command in the global configuration mode. To return to the global configuration mode, use the **no** form of this command.

evpn [{ **bgp** | **evi** | **interface** | **timers** }]
no evpn [{ **bgp** | **evi** | **interface** | **timers** }]

Syntax Description

bgp	Configures BGP.
evi	Configures Ethernet VPN ID (EVI).
interface	Assigns an interface to EVPN.
timers	Configures global EVPN timers.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enter the EVPN configuration mode:

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

host mac-address duplicate-detection

To enable duplicate detection of host MAC address, use the **host mac-address duplicate-detection** command in the EVPN configuration mode.

host mac-address duplicate-detection [**freeze-time** *freeze-time* | **move-count** *move-count* | **move-interval** *move-interval* | **retry-count** *retry-count* | **infinity** | **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 an MAC address before freezing it permanently. Default is three times.
infinite	Infinite retry count. Prevents freezing of the duplicate MAC address permanently.
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 addresses.

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enable duplicate detection of host MAC address:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host MAC-address duplicate-detection
Router(config-evpn-host-mac-addr-dup-detection)# move-count 2
Router(config-evpn-host-mac-addr-dup-detection)# freeze-time 10
Router(config-evpn-host-mac-addr-dup-detection)# retry-count 2
Router(config-evpn-host-mac-addr-dup-detection)# commit
```

This example shows how to prevent permanent freezing of duplicate host MAC address:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host MAC-address duplicate-detection
Router(config-evpn-host-mac-addr-dup-detection)# retry-count infinity
Router(config-evpn-host-mac-addr-dup-detection)# commit
```

This example shows how to reset the interval after which the count of duplicate detection events are permanently frozen.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host MAC-address duplicate-detection
Router(config-evpn-host-mac-addr-dup-detection)# reset-freeze-count-interval 20
Router(config-evpn-host-mac-addr-dup-detection)# commit
```

show bgp l2vpn evpn

To display BGP routes associated with EVPN under L2VPN address family, use the **show bgp l2vpn evpn** command in EXEC mode.

show bgp l2vpn evpn {**bridge-domain** *bridge-domain-name* | **rd** {**all** *IPv4 address:nn 4-byte as-number:nn 2-byte as-number:nn*}}

Syntax Description

bridge-domain *bridge-domain-name*	Displays the bridges by the bridge ID. The bridge-domain-name argument is used to name a bridge domain.
rd	Displays routes with specific route distinguisher.
all	Displays specified routes in all RDs.
IPv4 address:nn	Specifies the IPv4 address of the route distinguisher. nn: 16-bit number
4-byte as-number:nn	Specifies 4-byte AS number in asdot (X.Y) format or in asplain format. • For 4-byte AS number in asdot (X.Y) format, the range is from 1 to 65535. The format is: <1-65535>.<0-65535>:<0-65535> • For 4-byte AS number in asplain format, the range is from 65536 to 4294967295. The format is: <65536-4294967295>: nn: 32-bit number
2-byte as-number:nn	Specifies 2-byte as-number. The range is from 1 to 65535. nn: 32-bit number

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
bgp	read

Example

This sample output shows the BGP routes associated with EVPN with bridge-domain filter:

```
show bgp l2vpn evpn bridge-domain bd1
Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 192.0.2.1:1 (default for vrf bd1)
*>i[1][0077.0000.0000.0000.0001][0]/120
                      198.51.100.1                100      0 i
*>i[1][0077.0000.0000.0000.0001][4294967295]/120
                      198.51.100.1                100      0 i
*>i[1][0088.0000.0000.0000.0001][0]/120
                      203.0.113.1                 100      0 i
* i                   209.165.200.225             100      0 i
*>i[1][0088.0000.0000.0000.0001][4294967295]/120
                      203.0.113.1                 100      0 i
* i                   209.165.200.225             100      0 I
*  [2][0][48][0001.0000.0001][0]/104
*>                    209.165.201.1                        0 101 i
*>i[2][0][48][0002.0000.0001][0]/104
                      203.0.113.1                 100      0 102 i
* i                   209.165.200.225             100      0 102 i
*>i[3][0][32][203.0.113.1]/80
                      203.0.113.1                 100      0 i
*>i[3][0][32][209.165.200.225]/80
                      209.165.200.225             100      0 i
```

show evpn ethernet-segment

To display the EVPN Ethernet segment information, use the **show evpn ethernet-segment** command in the EXEC mode.

show evpn ethernet-segment [{ **detail** | **esi** | **interface** | **location** | **private** | **standby** | **carving** }]

Syntax Description

detail	Displays detailed information.
esi	Filters by Ethernet Segment identifier.
interface	Filters by interface name.
location	Displays location specific information.
private	Displays private information.
standby	Displays standby node specific information.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN Ethernet segment detailed information:

```
Router# show evpn ethernet-segment interface HundredGigE 0/0/0/24 detail

Ethernet Segment Id    Interface            Nexthops
--------------------   ----------           ----------
N/A                    HundredGigE 0/0/0/24 10.0.0.1
...............
Topology :
Operational : SH
```

show evpn evi

To display the EVPN E-VPN ID information, use the **show evpn evi** command in the EXEC mode.

show evpn evi [{ **bridge-domain** | **detail** | **inclusive-multicast** | **location** | **mac** | **standby** | **vpn-id** }]

Syntax Description

bridge-domain	Displays information for a specified bridge-domain..
detail	Displays detailed information.
inclusive-multicast	Displays EVPN Inclusive Multicast information.
location	Displays location specific information.
mac	Displays EVI MAC route associated configuration information.
standby	Displays standby node specific information.
vpn-id	Displays information for a specified E-VPN Identifier.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN EVI information with the VPN-ID and MAC address filter:

```
Router#show evpn evi vpn-id 185 mac 0024.be03.ce01
MAC address    Nexthop                                  Label    vpn-id
-------------- ---------------------------------------- -------- --------
0024.be03.ce01 3.100.100.100                            16004    185
               4.100.100.100                            16004    185
   ESI port key : 0x0000
   Source       : Remote
   Flush Count  : 0
```

This sample output shows the EVPN EVI information with the VPN-ID and inclusive-multicast filter:

```
Router#show evpn evi vpn-id 185 inclusive-multicast service-id 1850312 orig-ip 1.100.100.100
ISID           Originating IP                 vpn-id
-------------- ------------------------------ ----------
1850312        1.100.100.100                            185
1850312        2.100.100.100                            185
1850312        3.100.100.100                            185
1850312        4.100.100.100                            185
```

This sample output shows the EVPN EVI inclusive-multicast information:

```
Router#show evpn evi inclusive-multicast detail
ISID: 1850312, Originating IP: 1.100.100.100                            185
    Nexthop: ::
    Label  : 16005
    Source : Local
ISID: 1850312, Originating IP: 2.100.100.100                            185
    Nexthop: 2.100.100.100
    Label  : 16005
    Source : Remote
ISID: 1850312, Originating IP: 3.100.100.100                            185
    Nexthop: 3.100.100.100
    Label  : 16005
    Source : Remote
ISID: 1850312, Originating IP: 4.100.100.100                            185
    Nexthop: 4.100.100.100
    Label  : 16005
    Source : Remote
```

This sample output shows the EVPN EVI information with the bridge-domain filter:

```
Router#show evpn evi bridge-domain tb1-core1 detail
EVI        Bridge Domain                Type
---------- ---------------------------- -------
145        tb1-core1                    PBB
165        tb1-core2                    PBB
185        tb1-core3                    PBB
65535      ES:GLOBAL                    BD
```

This sample output shows the EVPN EVI detailed information:

```
Router#show evpn evi detail
EVI        Bridge Domain                Type
---------- ---------------------------- -------
145        tb1-core1                    PBB
   Unicast Label  : 16000
   Multicast Label: 16001
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:145
   RT Auto  : 100:145
   Route Targets in Use           Type
   ------------------------------ -------
   100:145                        Import
   100:145                        Export

165        tb1-core2                    PBB
```

```
   Unicast Label  : 16002
   Multicast Label: 16003
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:165
   RT Auto  : 100:165
   Route Targets in Use           Type
   ------------------------------ -------
   100:165                        Import
   100:165                        Export

185        tb1-core3                    PBB
   Unicast Label  : 16004
   Multicast Label: 16005
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:185
   RT Auto  : 100:185
   Route Targets in Use           Type
   ------------------------------ -------
   100:185                        Import
   100:185                        Export

65535      ES:GLOBAL                    BD
   Unicast Label  : 0
   Multicast Label: 0
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:0
   RT Auto  : none
   Route Targets in Use           Type
   ------------------------------ -------
   0100.9e00.0210                 Import
   0100.be01.ce00                 Import
   0100.be02.0101                 Import
```

show evpn summary

To display the EVPN summary, use the **show evpn summary** command in the EXEC mode.

show evpn summary[{**location** | **private** | **standby**}]

Syntax Description

location	Displays location specific information.
private	Displays private information.
standby	Displays standby node specific information.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN summary:

```
Router#show evpn summary
-----------------------------
Global Information
-----------------------------
Number of EVIs                 : 1
Number of Local MAC Routes     : 1
Number of Remote MAC Routes    : 0
Number of Local IMCAST Routes  : 0
Number of Remote IMCAST Routes: 0
Number of Internal Labels      : 0
Number of ES Entries           : 0
BGP Router ID                  : ::
BGP ASN                        : Invalid
PBB BSA MAC address            : f866.f214.abd7
Global peering timer           :     45 seconds
Global recovery timer          :     20 seconds
Global programming timer       :   1500 microseconds
Global flushagain timer        :     60 seconds
-----------------------------
High Availability Information
```

```
-----------------------------
BGP EOD                       : N
Number of Marked MAC Routes   : 0
Number of Swept MAC Routes    : 0
Number of Marked IMCAST Routes: 0
Number of Swept IMCAST Routes : 0
```

L2VPN Commands

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

By default, all interfaces are Layer 3 interfaces. You can change the interface to Layer 2 interface using the **l2transport** command.

For detailed information about concepts and configuration, see the *Introduction to Layer 2 Virtual Private Networks* chapter in the L2VPN and Ethernet Services Configuration Guide for Cisco 8000 Series Routers.

bridge-domain

To establish a bridge domain and to enter L2VPN bridge group bridge domain configuration mode, use the **bridge-domain** command in L2VPN bridge group configuration submode.

bridge-domain *bridge-domain-name*

Syntax Description

bridge-domain-name	Name of the bridge domain. **Note** The maximum number of characters that can be specified in the bridge domain name is 27.

Command Default

The default value is a single bridge domain.

Command Modes

L2VPN bridge group configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

Use the **bridge-domain** command to enter L2VPN bridge group bridge domain configuration mode.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure a bridge domain:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group BG1
Router(config-l2vpn-bg)# bridge-domain BD1
Router(config-l2vpn-bg-bd)#
```

Related Commands

Command	Description
l2vpn, on page 28	Enters L2VPN configuration mode.
bridge group, on page 21	Creates a bridge group
show l2vpn bridge-domain, on page 34	Display information for the bridge ports such as attachment circuits for the specific bridge domains.

bridge group

To create a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain, use the **bridge group** command in L2VPN configuration mode. To remove all the bridge domains that are created under this bridge group and to remove all network interfaces that are assigned under this bridge group, use the **no** form of this command.

bridge group *bridge-group-name*
no bridge-group *bridge-group-name*

Syntax Description

bridge-group-name	Number of the bridge group to which the interface belongs.

Command Default

No bridge group is created.

Command Modes

L2VPN configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

Use the **bridge group** command to enter L2VPN bridge group configuration mode.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows that bridge group 1 is assigned:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group BG1
Router(config-l2vpn-bg)#
```

Related Commands

Command	Description
l2vpn, on page 28	Enters L2VPN configuration mode.
bridge-domain, on page 20	Establishes a bridge domain

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.

encapsulation **dot1ad** *vlan-id*

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 7.3.2	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 HundredGigE 0/0/0/24.1 l2transport
Router(config-subif)# encapsulation dot1ad 10
```

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.

encapsulation **dot1q** *vlan-id*

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 7.3.2	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 HundredGigE 0/0/0/24.1 l2transport
Router(config-subif)# encapsulation dot1q 10
```

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 interface configuration mode. To remove the configuration, use the **no** form of this command.

encapsulation **dot1q** *vlan-id* [{ **second-dot1q** *vlan-id* }]

Syntax Description

vlan-id	Specifies VLAN identifier.
dot1q	Specifies IEEE 802.1Q VLAN tagged packets.
second-dot1q	

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 24.1.1	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.
- Only one encapsulation command must be configured per VLAN service instance.
- Overlapping inner VLAN ranges are not supported.

Examples

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

```
Router#configure
Router(config)#interface TenGigE 0/0/0/1.102 l2transport
Router(config-subif)#encapsulation dot1q 200 second-dot1q 201
Router(config-subif)#commit
Router(config-subif)#exit
Router(config)#exit
```

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.

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 7.11.1	This command was introduced.

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
```

interface

To create a VLAN interface or subinterface, use the **interface** command in global configuration mode.

interface *type* *interface-path-id* **.** *subinterface*

Syntax Description

type	Type of Ethernet interface on which you want to create a VLAN interface or subinterface. Enter **HundredGigabitEthernet**.
interface-path-id	Physical interface or virtual interface followed by the interface path ID. Naming notation is *interface-path-id*. For more information about the syntax for the router, use the question mark (?) online help function.
subinterface	Physical interface or virtual interface followed by the subinterface path ID. Naming notation is *interface-path-id.subinterface*. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.
  - *port*: Physical port number of the interface.
- If specifying an Ethernet bundle interface, the range is from 1 through 65535.

For the *subinterface* argument, the range is from 0 through 4095.

To configure a large number of subinterfaces, we recommend entering all configuration data before you commit the **interface** command.

Usage Guidelines

Note A subinterface does not pass traffic without an assigned VLAN ID.

Task ID

Task ID	Operations
vlan	read, write

Examples

This example shows how to configure a VLAN interface on a 100-Gigabit Ethernet interface:

```
Router# configure
Router(config)# interface HundredGigE 0/0/0/24
Router(config-subif)# dot1q vlan 1
Router(config-subif)# ipv4 address 10.0.0.1/8
```

This example shows how to configure a VLAN subinterface on a 100-Gigabit Ethernet interface:

```
Router# configure
Router(config)# interface HundredGigE 0/0/0/24.1
Router(config-subif)# dot1q vlan 1
Router(config-subif)# ipv4 address 10.0.0.1/8
```

To change an interface from Layer 2 to Layer 3 mode and back, you must delete the interface first and then re-configure it in the appropriate mode.

```
Router# configure
Router(config)# interface HundredGigE 0/0/0/24
Router(config-subif)# exit
Router(config)# no interface HundredGigE 0/0/0/24
```

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

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.2.12	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)#
```

Related Commands

Command	Description
show l2vpn, on page 33	Displays L2VPN information

mac withdraw

To enable MAC address withdrawal for a specified bridge domain, use the **mac withdraw** command in L2VPN configuration mode.

mac withdraw [**disable** | **optimize** | **state-down**]

Syntax Description

disable	Disables MAC address withdrawal.
optimize	Enables optimization of MAC address withdrawal when the bridge port goes down.
state-down	Sends MAC address withdrawal message when the bridge port goes down.

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

The following example shows how to disable MAC address withdrawal.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw disable
```

The following example shows how to configure MAC address withdrawal when the bridge port goes down.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw state-down
```

The following example shows how to configure optimization of MAC address withdrawal when the bridge port goes down.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw optimize
```

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** | | **load-balancing flow-label** | **both** }
pw-class *class-name* **encapsulation mpls** { **control-word** | | **load-balancing flow-label** | **both** }

Syntax Description

class-name	Encapsulation class name.
control-word	Disables control word for MPLS encapsulation. Disabled by default.
load-balancing flow-label both	Sets flow-label based load balancing.

Command Default

None

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 7.3.15	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 path1
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# control-word
Router(config-l2vpn-pwc-mpls)# load-balancing flow-label both
```

rewrite ingress tag

To specify the encapsulation adjustment that is to be performed on the frame ingress to the VLAN service instance, use the **rewrite ingress tag** command in the interface configuration mode. Use the following VLAN rewrite configuration to add or modify double dot1q VLAN tags on L2 Ethernet frames. To delete the encapsulation adjustment, use the **no** form of this command.

rewrite ingress tag {**push** {**dot1q** *vlan-id*} | **pop** { **2** } | **translate** {**1-to-2** { **dot1q** *vlan-id* **second-dot1q** *vlan-id* } | **2-to-2** { **dot1q** *vlan-id* **second-dot1q** *vlan-id* }}} [**symmetric**]

Syntax Description

vlan-id	Specifies VLAN identifier.
push dot1q *vlan-id* **second-dot1q** *vlan-id*	Pushes the pair of 802.1Q tags with VLAN IDs.
pop {2}	Specifies removal of the pair of 802.1Q tags from the packet.
translate 1-to-2 dot1q *vlan-id* **second-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.
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 Dot1q VLAN tags in the Ethernet frame is not modified on ingress.

Command Modes

Interface configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

The **symmetric** keyword is accepted only when a single VLAN is configured in encapsulation.

Define the elements being popped with an encapsulation type before using the **pop** command.

Define the elements being translated with an encapsulation type before using the **rewrite ingress tag translate** command. In the 2-to-1 option, “2” means two tags of a type defined by the **encapsulation** command.

Examples

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

```
Router#configure
Router(config)#interface TenGigE 0/0/0/1.102 l2transport
Router(config-subif)#encapsulation dot1q 200 second-dot1q 201
Router(config-subif)#rewrite ingress tag pop 2 symmetric
Router(config-subif)#commit
Router(config-subif)#exit
Router(config)#exit
```

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 7.2.12	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 28	Enters L2VPN configuration mode.

show l2vpn bridge-domain

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

show l2vpn bridge-domain [{ **autodiscovery bgp** | **bd-name bridge-domain-name** | **brief** | **detail** | **group bridge-domain-group-name** | **hardware** | **interface** *type interface-path-id* | **location** *node-id* **neighbor** *ip-address* | **summary** | **no-statistics** | **p2mp tunnel-id** *id* | **standby** }]

Syntax Description

autodiscovery bgp	(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 AC.
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.
location*node-id*	(Optional) Displays the location specific information of the node.
neighbor *ip-address*	(Optional) Displays the bridge domains that contain the ACs to match the filter for the neighbor. The *ip-address* argument is used to specify IP address of the neighbor.
no-statistics	(Optional) Disables the collection of statistics for the bridge domain.
p2mp tunnel-id *id*	(Optional) Displays the bridge domain that contain the p2mp enabled bridge domain. The **tunnel-id** *id* argument is used too specify the tunnel of the p2mp brigde domain.
summary	(Optional) Displays the summary information for the bridge domain.
standby	(Optional) Displays whether the node is in the standby mode.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

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.

Task ID

Task ID	Operations
l2vpn	read

Examples

This is the sample output for **show l2vpn bridge-domain** command with VLAN parameters configured:

```
Router# show l2vpn bridge-domain bd-name BG1_BD1 detail
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: bg1_bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  Coupled state: disabled
  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: 4000, Action: none, Notification: syslog
  MAC limit reached: no
  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
  IGMP Snooping: enabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
  Storm Control: disabled
  Bridge MTU: 1500
  MIB cvplsConfigIndex: 1
  Filter MAC addresses:
  P2MP PW: disabled
  Create time: 30/03/2015 22:25:38 (00:26:08 ago)
  No status change since creation
  ACs: 2 (2 up), VFIs: 1, PWs: 0 (0 up), PBBs: 0 (0 up)
  List of ACs:
    AC: BVI1, state is up
      Type Routed-Interface
      MTU 1514; XC ID 0x80000001; interworking none
      BVI MAC address:
        1000.4444.0001
    AC: HundredgiabitEthernet0/0/0/0.1, state is up
      Type VLAN; Num Ranges: 1
      Outer Tag: 1
      VLAN ranges: [1001, 1001]
      MTU 1508; XC ID 0x508000a; interworking none
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: no
      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
      IGMP Snooping: enabled
      IGMP Snooping profile: none
      MLD Snooping profile: none
      Storm Control: bridge-domain policer
      Static MAC addresses:

      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
  List of VNIs:
    VNI 1, state is up
      XC ID 0x80000014
      Encap type VXLAN
      Overlay nve100, Source 10.0.0.1, Multicast Group 225.1.1.1, UDP Port 4789
      Anycast VTEP 100.1.1.1, Anycast Multicast Group 224.10.10.1
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: no
      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
      IGMP Snooping: enabled
      IGMP Snooping profile: none
      MLD Snooping profile: none
      Storm Control: bridge-domain policer

  List of Access PWs:
  List of VFIs:
    VFI bg1_bd1_vfi (up)
      VFI Statistics:
        drops: illegal VLAN 0, illegal length 0
```

Verify the EVPN and VPLS status.

```
Router# show l2vpn bridge-domain
Legend: pp = Partially Programmed.
Bridge group: vplstoevpn, bridge-domain: vplstoevpn, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 2 (1 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of EVPNs:
    EVPN, state: up
  List of ACs:
    Hu0/0/0/0, state: up, Static MAC addresses: 0, MSTi: 5
  List of Access PWs:
  List of VFIs:
    VFI vpls (up)
      Neighbor 172.16.0.1 pw-id 12, state: down, Static MAC addresses: 0
      Neighbor 192.168.0.1 pw-id 13, state: up, Static MAC addresses: 0
```

This indicates that VPLS and EVPN L2 bridging for the same VPN instance coexists and EVPN takes precedence over VPLS.

Related Commands

Command	Description
l2vpn, on page 28	Enters L2VPN configuration mode.
show l2vpn, on page 33	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 7.2.12	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
```

```
HundredGigE0/0/0/0.1:
      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: HundredGigE0_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 28	Enters L2VPN configuration mode.
show l2vpn, on page 33	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 7.2.12	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
------------------------------------ ------------------------------------ ------
Hu0/0/0/0.234                        ac Hu0/0/0/26.234                    UP
Hu0/0/0/0.233                        ac Hu0/0/0/26.233                    UP
Hu0/0/0/0.232                        ac Hu0/0/0/26.232                    UP
Hu0/0/0/0.231                        ac Hu0/0/0/26.231                    UP
Hu0/0/0/0.230                        ac Hu0/0/0/26.230                    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
---------------------------------- ---------------------------------- -- ---------
Hu0/0/0/0.234                      ac Hu0/0/0/26.234                  UP 15098997504
Hu0/0/0/0.233                      ac Hu0/0/0/26.233                  UP 15098997568
Hu0/0/0/0.232                      ac Hu0/0/0/26.232                  UP 15098997504
Hu/0/0/0.231                       ac Hu0/0/0/26.231                  UP 15098997568
HU0/0/0/0.230                      ac Hu0/0/0/26.230                  UP 15098997568
```

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

```
Router# show l2vpn forwarding summary location 0/RP0/CPU0
 Thu Oct 22 06:14:17.767 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:721, minor version num:2
Shared memory timestamp:0x19c9b0f580
Global configuration:
Number of forwarding xconnect entries:0
  Up:0  Down:0
  AC-PW(atom):0 AC-PW(iid):0 AC-PW(l2tpv2):0 AC-PW(l2tpv3):0
  AC-PW(l2tpv3-ipv6):0
  AC-AC:0  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
 0 Global
  Exceeded max allowed: 0 VPLS PW, 0 Bundle-AC
Number of p2p xconnects: 0
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 ipmacs: 0
  0 Locally learned ip4macs
  0 Remotely learned ip4macs
  0 Locally learned ip6macs
  0 Remotely learned ip6macs
Number of total P2MP Ptree entries: 0
Number of PWHE Main-port entries: 0
Number of EVPN Multicast Replication lists: 0 (0 default, 0 stitching, 0 isid)
```

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: HundredGigE 0/0/0/24, Xconnect id: 0x1, Status: up
  Segment 1
    AC, HundredGigE 0/0/0/24, 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, HundredGigE 0/0/0/24, status: Bound

Local interface: HundredGigE 0/0/0/25, Xconnect id: 0x2, Status: up
  Segment 1
    AC, HundredGigE 0/0/0/25, 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, HundredGigE 0/0/0/25, status: Bound

Local interface: HundredGigE 0/0/0/24, Xconnect id: 0x3, Status: up
 Segment 1
    AC, HundredGigE 0/0/0/24, 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, HundredGigE 0/0/0/24, status: Bound
```

Related Commands

Command	Description
l2vpn, on page 28	Enters L2VPN configuration mode.
show l2vpn, on page 33	Displays L2VPN information
show l2vpn database, on page 38	Displays L2VPN database

show l2vpn protection main-interface

To display an overview of the main interface or instance operational information, use the **show l2vpn protection main-interface** command in EXEC mode.

show l2vpn protection main-interface [*interface name* { *Interface* }] [{ **brief** | **detail** | **private** }]

Syntax Description

interface name	Interface name of the Ethernet ring G.8032 name.
interface	The forwarding interface ID in number or in Rack/Slot/Instance/Port format as required.
brief	Brief information about the G.8032 ethernet ring configuration.
detail	Information in detail about the G.8032 ethernet ring configuration.
private	Private information about the G.8032 ethernet ring configuration.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.2.12	This command was introduced.
Release 7.7.1	The command output was enhanced to include protection access gateway subtype indication `MST-AG`.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This example shows the output from the **show l2vpn protection main-interface** command:

```
RP/0/0/CPU0:router# show l2vpn protection main-interface

Main Interface ID              Subintf Count Protected  Blocked
------------------------------ ------------- ---------- ----------
GigabitEthernet0/0/0/0         1             None       No
```

```
   Instance : 0
      State         : FORWARDING
      Sub-Intf #    : 1
      Flush    #    : 0
       Sub-interfaces : GigabitEthernet0/0/0/0.4


Main Interface ID              Subintf Count Protected  Blocked
------------------------------ ------------- ---------- ----------
GigabitEthernet0/0/0/1         1             None       No
   Instance : 0
      State         : FORWARDING
      Sub-Intf #    : 1
      Flush    #    : 0
       Sub-interfaces : GigabitEthernet0/0/0/0.4

RP/0/0/CPU0:ios#show l2vpn protection main-interface gigabitEthernet 0/0/0/1
Tue Mar 15 10:54:13.366 EDT
Main Interface ID              # of subIntf Protected  Protect Type
------------------------------ ------------ ---------- ------------
GigabitEthernet0/0/0/1         2            Yes        MST-AG

   Instance : 0
      State          : FORWARDING
      Sub-Intf #     : 1
      Flush    #     : 1

   Instance : 1
      State          : BLOCKED
      Sub-Intf #     : 1
      Flush    #     : 0

RP/0/0/CPU0:ios#show l2vpn protection main-interface gigabitEthernet 0/0/0/2
Tue Mar 15 10:54:15.044 EDT
Main Interface ID              # of subIntf Protected  Protect Type
------------------------------ ------------ ---------- ------------
GigabitEthernet0/0/0/2         2            Yes        STP

   Instance : 0
      State          : FORWARDING
      Sub-Intf #     : 1
      Flush    #     : 0

   Instance : 1
      State          : FORWARDING
      Sub-Intf #     : 1
      Flush    #     : 0

RP/0/0/CPU0:router# show l2vpn protection main-interface brief

Main Interface ID              Ref Count  Instance   Protected  State
------------------------------ ---------- ---------- ---------  -----
GigabitEthernet0/0/0/0         3          2          No     FORWARDING
GigabitEthernet0/0/0/1         1          1          No     FORWARDING


RP/0/RSP0/CPU0:router# show l2vpn protection main-interface detail

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/19        4            No

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
```

```
GigabitEthernet0/1/0/20        3            No

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/3         2            No

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/30        1            No

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/7         4            No


RP/0/0/CPU0:router# show l2vpn protection main-interface private

Main Interface ID              Ref Count  Protected  Blocked    If Handle  Registered
------------------------------ ---------- ---------- ---------- ---------- ----------
GigabitEthernet0/0/0/0         3          None       No         0x20000020 No

   Instance : 0
      State          : FORWARDING        Config ID  : 0
      Sub-Intf #     : 0                 Ack      # : 0
      Bridge D #     : 0                 N-Ack    # : 0
      Flush    #     : 0                 Rcv      # : 0
      Sub-interfaces : GigabitEthernet0/0/0/0.4

     Instance event trace history [Total events: 1, Max listed: 8]
     --------------------------------------------------------
     Time                Event                          State           Action
     ====                =====                          ========        ========
     01/01/1970 01:00:01 Rcv state IF known             Invalid         134833160
     07/02/2010 10:13:03 Update L2FIB                   FORWARDING      0
     01/01/1970 01:00:25 Rcvd AC MA create + UP I/F ST  FORWARDING      0
```

Related Commands

Command	Description
l2vpn	Enters L2VPN configuration mode.

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 7.2.12	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 a sample output for the **show l2vpn resource** command:

```
Router# show l2vpn resource
Wed Oct 14 11:27:23.447 UTC
Memory: Normal
```

This table describes the significant fields shown in the display.

Table 2: show l2vpn resource Command Field Descriptions

Field	Description
Memory	Displays memory status.

Related Commands

Command	Description
l2vpn, on page 28	Enters L2VPN configuration mode.
show l2vpn, on page 33	Displays L2VPN information

show l2vpn trace

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

show l2vpn trace [**checker**] | [**file** *filename* *filepath*] | [**last** *entry*] | [**location** *node-id*] | [**udir** *path*] [**reverse**] | [**stats**] | [**tailf**] | [**usec**] | [**verbose**] | [**wide**]

Syntax Description

checker	Displays trace data for the L2VPN Uberverifier.
file *filename filepath*	Displays trace data for the specified file.
hexdump	Display traces data in hexadecimal format.
last *entry*	Display last <n> entries
location *node-id*	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
udir *path*	Display a temporary directory to copy traces from remote locations
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 7.2.12	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 28	Enters L2VPN configuration mode.
show l2vpn, on page 33	Displays L2VPN information
show l2vpn resource, on page 47	Displays the memory state in the L2VPN process.

split-horizon group

To add an AC to a split horizon group, use the **split-horizon group** command in L2VPN bridge group bridge domain attachment circuit configuration mode.

split-horizon group

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN bridge group bridge domain attachment circuit configuration mode

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

Only one split horizon group exists for ACs per bridge domain. By default, the group does not have any ACs. You can configure individual ACs to become members of the group using the **split-horizon group** configuration command.

You can configure an entire physical interface or EFPs within an interface to become members of the split horizon group.

Task ID

Task ID	Operations
l2vpn	Read, write

Examples

The following example shows the split horizon group configuration:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg
Router(config-l2vpn-bg)# bridge-domain bd
Router(config-l2vpn-bg-bd-ac)# interface Ten0/7/0/22/0 <- (split-horizon group 0, default)
Router(config-l2vpn-bg-bd-ac)# interface Ten0/7/0/22/1.1
Router(config-l2vpn-bg-bd-ac)# split-horizon group <- (split-horizon group 2)
Router(config-l2vpn-bg-bd-ac)# neighbor 10.0.0.1 pw-id 1
Router(config-l2vpn-bg-bd-pw)# split-horizon group <- (split-horizon group 2)
Router(config-l2vpn-bg-bd-pw)# vfi vf
Router(config-l2vpn-bg-bd-vfi)# neighbor 172.16.0.1 pw-id 10001 <- (split-horizon group 1,
 default)
Router(config-l2vpn-bg-bd-vfi-pw)# commit
```

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 7.3.2	This command was introduced.

Usage Guidelines

- Storm control is supported on main ports only.
- Storm control configuration is supported at the bridge-port level, and not at the bridge-domain level.
- PW-level storm control is not supported.
- Storm control is not supported through QoS input policy.
- Although pps is configurable, it is not natively supported. PPS configuration is converted to a kbps value assuming a 256 byte packet size when configuring the hardware policers.

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 BG1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain BD1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface HundredGigE0/0/0/0
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
```

vpws-seamless-integration

To enable EVPN-VPWS seamless integration, use the **vpws-seamless-integration** command in L2VPN configuration mode. To disable EVPN-VPWS seamless integration, use the **no** form of this command.

vpws-seamless-integration

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 7.8.1	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 EVPN-VPWS integration on an edge device for BGP PW.

```
Router# configure
Router(config)# l2vpn xconnect group 1
Router(config-l2vpn-xc)# mp2mp 2
Router(config-l2vpn-xc-mp2mp)# autodiscovery bgp
Router(config-l2vpn-xc-mp2mp-ad)# signaling-protocol bgp
Router(config-l2vpn-xc-mp2mp-ad-sig)# ce-id 3
Router(config-l2vpn-xc-mp2mp-ad-sig-ce)# vpws-seamless-integration
```

The following example shows how to enable EVPN-VPWS integration for TLDP PW.

```
Router# configure
Router(config)# l2vpn xconnect group 1
Router(config-l2vpn-xc)# p2p p1
Router(config-l2vpn-xc-p2p)# interface BE1.1
Router(config-l2vpn-xc-p2p)# neighbor 1.1.1.1 pw-id 1
Router(config-l2vpn-xc-p2p-pw)# exit
Router(config-l2vpn-xc-p2p)# vpws-seamless-integration
```

Multiple Spanning Tree Protocol Commands

This module describes the commands used to configure multiple spanning tree protocol. For detailed information about MSTP concepts, configuration tasks, and examples, see the *L2VPN and Ethernet Services Configuration Guide for Cisco 8000 Series Routers*.

instance (MSTP)

To enter the multiple spanning tree instance (MSTI) configuration submode, 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 7.2.12	This command was introduced.

Usage Guidelines

Note An instance ID of 0 represents the CIST for the region.

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
Router# configure
Router(config)#spanning-tree mst a
Router(config-mstp)# instance 101
Router(config-mstp-inst)#
```

Related Commands

Command	Description
show spanning-tree mst, on page 60	Displays the multiple spanning tree protocol status information.
spanning-tree mst, on page 62	Enters the MSTP configuration submode
vlan-id (MSTP), on page 63	Associates a set of VLAN IDs with the current MSTI.

interface (MSTP)

To enter the MSTP interface configuration submode, and to enable STP for the specified port, use the **interface** command in MSTP configuration submode.

interface ***interface-type interface-path-id***

Syntax Description

interface	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface. 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 7.2.12	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# configure
Router(config)# spanning-tree mst M0
Router(config-mstp)# interface hundredGigE 0/0/0/1
Router(config-mstp-if)#
```

Related Commands

Command	Description
show spanning-tree mst, on page 60	Displays the multiple spanning tree protocol status information.
spanning-tree mst, on page 62	Enters the MSTP configuration submode

name (MSTP)

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

name *name*

Syntax Description

name	Specifies the name of the mstp region. 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 7.2.12	This command was introduced.

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
Router# configure
RP/0/RP0/CPU0:ios(config)#spanning-tree mst M0
Router(config-mstp)# name m1
```

Related Commands

Command	Description
show spanning-tree mst, on page 60	Displays the multiple spanning tree protocol status information.
spanning-tree mst, on page 62	Enters the MSTP configuration submode

portfast

To enable Port Fast on the port, and optionally 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 7.2.12	This command was introduced.

Usage Guidelines

You must disable and re-enable the port for Port Fast configuration to take effect. Use **shutdown** and **no shutdown** command (in interface configuration mode) to disable and re-enable the port.

This command enables the Port Fast 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. For more information on Port Fast feature, refer to the *Multiple Spanning Tree Protocol* module in the *L2VPN and Ethernet Services Configuration Guide for Cisco 8000 Series Routers*

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
Router# configure
Router(config)# spanning-tree mst a
Router(config-mstp)# interface HundredGigE0/0/0/2
Router(config-mstp-if)# portfast
Router(config-mstp-if)# portfast bpduguard
```

Related Commands

Command	Description
interface (MSTP), on page 57	Enters the MSTP interface configuration submode, and enables STP for the specified port.
show spanning-tree mst, on page 60	Displays the multiple spanning tree protocol status information.
spanning-tree mst, on page 62	Enters the MSTP configuration submode

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 7.2.12	This command was introduced.

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:

```
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
```

```
----------------------   -------- ------ ---------   ------------------------ --------
HundredGigEthernet0/0/0/1   128.65   20000  DSGN FWD    0    4097 0004.9b78.0800 128.65
HundredGigEthernet0/0/0/2   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:

```
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 HundredGigEthernet0/0/0/2  , Root Bridge ID 0002.9b78.0812
...
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
----------------------   -------- ------ ---------   ------------------------ --------
HundredGigEthernet0/0/0/4      128.196  200000 ALT  BLK    0    4097 0004.9b78.0800 128.195

...
```

Related Commands

Command	Description
spanning-tree mst, on page 62	Enters the MSTP configuration submode

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 7.2.12	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 a
Router(config-mstp)#
```

Related Commands

Command	Description
instance (MSTP), on page 56	Enters the multiple spanning tree instance (MSTI) configuration submode.
interface (MSTP), on page 57	Enters the MSTP interface configuration submode, and enables STP for the specified port.
show spanning-tree mst, on page 60	Displays the multiple spanning tree protocol status information.

vlan-id (MSTP)

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

vlan-id *vlan-range* [*vlan-range*] [*vlan-range*] [*vlan-range*]

Syntax Description

vlan-range	List of VLAN ranges in the form a-b, c, d, e-f, g etc.

Command Default

None

Command Modes

MSTI configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
Router(config-mstp-inst)# vlan-id 2-1005
```

Related Commands

Command	Description
instance (MSTP), on page 56	Enters the multiple spanning tree instance (MSTI) configuration submode.
spanning-tree mst, on page 62	Enters the MSTP configuration submode
show spanning-tree mst, on page 60	Displays the multiple spanning tree protocol status information.

Integrated Routing and Bridging Commands

This module describes the commands to configure Integrated Routing and Bridging (IRB) on the Cisco 8000 Series Routers.

interface bvi

To create a bridge-group virtual interface (BVI), use the **interface bvi** command in Global Configuration mode. To delete the BVI, use the **no** form of this command.

interface **bvi** *identifier*

Syntax Description

identifier	Number for the BVI interface from 1 to 4294967295.

Command Default

No BVI interface is configured.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

The BVI is a virtual interface within the router that acts like a normal routed interface. The BVI does not support bridging itself, but acts as a gateway for the corresponding bridge-domain to a routed interface within the router.

Aside from supporting a configurable MAC address, a BVI supports only Layer 3 attributes, and has the following characteristics:

- Uses a MAC address taken from the local chassis MAC address pool, unless overridden at the BVI interface.
- Is configured as an interface type using the **interface bvi** command and uses an IPv4 or IPv6 address that is in the same subnet as the hosts on the segments of the bridged domain. The BVI also supports secondary addresses.
- The BVI identifier is independent of the bridge-domain identifier. These identifiers do not need to correlate like they do in Cisco IOS software.
- Is associated to a bridge group using the **routed interface bvi** command.
- The following interface commands are supported on a BVI:
    - **arp purge-delay**
    - **arp timeout**
    - **bandwidth** (The default is 10 Gbps and is used as the cost metric for routing protocols for the BVI.)
    - **ipv4**
    - **ipv6**
    - **mac-address**
    - **mtu** (The default is 1514 bytes.)
    - **shutdown**

- The BVI supports IP helper addressing and secondary IP addressing.

To display bridge group, bridge-domain, interface status, line protocol state, and packet counters for the specified BVI, use the **show l2vpn bridge domain interface bvi** form of the **show l2vpn bridge domain (VPLS)** command. To display the reason that a BVI is down, you can use the **detail** keyword option.

Task ID

	Operations
interface	read, write

Examples

The following example shows how to create a BVI interface and configure its IPv4 address:

```
Router# configure
Router(config)# interface bvi 50
Router(config-if)# ipv4 address 10.10.0.4 255.255.255.0
Router(config-if)# commit
```

Related Commands

Command	Description
routed interface bvi , on page 68	
show interfaces bvi, on page 69	

routed interface bvi

To associate the specified bridge group virtual interface (BVI) as the routed interface for the interfaces assigned to the bridge domain, use the **routed interface bvi** command in L2VPN bridge group bridge domain configuration mode. To remove the BVI as the routed interface for the interfaces assigned to the bridge domain, use the **no** form of this command.

routed interface bvi *identifier*

Syntax Description

identifier	Number for the BVI interface from 1 to 65535.

Command Default

No routed interface is configured.

Command Modes

L2VPN bridge group bridge domain configuration mode (config-l2vpn-bg-bd)

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

- Only one BVI can be configured in any bridge domain.
- The same BVI can not be configured in multiple bridge domains.

Task ID

Task ID	Operation
l2vpn	read, write

The following example shows association of a BVI interface numbered “50” on the bridge domain named “IRB”:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 10
Router(config-l2vpn-bg)# bridge-domain IRB
Router(config-l2vpn-bg-bd)# routed interface bvi 50
Router(config-l2vpn-bg-bd-bvi)# commit
```

Related Commands

Command	Description
interface bvi , on page 66	
show interfaces bvi, on page 69	

show interfaces bvi

To display interface status, line protocol state, and packet counters for the specified BVI, use the **show interfaces bvi** command in XR EXEC mode.

show interfaces bvi *identifier* [**accounting** | **brief** | **description** | **detail** | **location** *location*]

Syntax Description

identifier	Number for the BVI interface from 1 to 4294967295.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
brief	(Optional) Displays summary information about the interface.
description	(Optional) Displays summary status information and the description for the interface.
detail	(Optional) Displays detailed information about the interface. This is the default.
location *location*	(Optional) Displays information the interface on the specified node. The *location* argument is entered in the *rack/slot/module* notation.

Command Default

Detailed information about the BVI interface is displayed.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	read

The following example shows sample output for the **show interfaces bvi** command:

```
Router# show interfaces bvi 50
Mon Oct 19 07:22:55.233 UTC
BVI50 is down, line protocol is down
  Interface state transitions: 0
  Hardware is Bridge-Group Virtual Interface, address is
  Internet address is 10.10.0.4/24
  MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,  loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
  Last input never, output never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
     0 packets output, 0 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
```

Table 3: show interfaces bvi Field Descriptions

Field	Description
BVI*x* is	Displays the state of the specified BVI interface, where *x* is the number of the interface. The possible values are: administratively down, down, or up.
line protocol is	Displays the stateof the line protocol for the BVI interface. The possible values are: administratively down, down, or up. **Note** The line protocol state is not the same as the protocol state displayed in the **show ip interfaces** command, because it is the state of Layer 2 (media) rather than Layer 3 (IP protocol).
Interface state transitions:	Displays the number of times the interface has changed states.
Hardware is	Displays Bridge-Group Virtual Interface for a BVI.
address is	Layer 2 MAC address of the BVI.
Description:	Displays the description of the interface when configured.
Internet address is *n.n.n.n*/*n*	Layer 3 IP address of the BVI in dotted decimal format.
MTU	Displays the maximum transmission unit (MTU) for the interface. The MTU is the maximum packet size that can be transmitted over the interface. 1514 is the default.
BW *x* Kbit	Displays the current bandwidth of the interface in kilobits per second.
Max:	Displays the maximum bandwidth available on the interface in kilobits per second.
reliability	Displays the proportion of packets that are not dropped and do not have errors. **Note** The reliability is shown as a fraction of 255.

Field	Description
txload	Indicates the traffic flowing out of the interface as a proportion of the bandwidth. **Note** The txload is shown as a fraction of 255.
rxload	Indicates the traffic flowing into the interface as a proportion of the bandwidth. **Note** The rxload is shown as a fraction of 255.
Encapsulation	Layer 2 encapsulation on the interface.
loopback	Always displays “not set” for a BVI because loopbacks are not supported.
ARP type	Address Resolution Protocol (ARP) type used on the interface.
ARP timeout	ARP timeout in the format hours:mins:secs. This value is configurable using the **arp timeout** command.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
Last clearing of “show interface” counters	Time since the counters in this command were last cleared using the **clear counters** Exec command in hours:mins:secs.

Field	Description
5 minute input rate	Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). **Note** The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes. **Note** The 5-minute input should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). **Note** The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes. **Note** The 5-minute output should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Number of packets received on the interface that were successfully delivered to higher layers.
bytes	Number of bytes received on the interface.

Field	Description
total input drops	Total number of valid packets that were dropped after they were received. This includes packets that were dropped due to configured quality of service (QoS) or access control list (ACL) policies. This does not include drops due to unknown Layer 3 protocol.
drops for unrecognized upper-level protocol	Total number of packets that could not be delivered because the necessary protocol was not configured on the interface.
Received *x* broadcast packets	Total number of Layer 2 broadcast packets received on the interface. This is a subset of the total input packet count.
multicast packets	Total number of Layer 2 multicast packets received on the interface. This is a subset of the total input packet count.
packets output	Number of packets sent from the interface.
bytes	Total number of bytes successfully sent from the interface.
total output drops	Number of packets that were dropped before being transmitted.
Output *x* broadcast packets	Number of Layer 2 broadcast packets transmitted on the interface. This is a subset of the total output packet count.
multicast packets	Total number of Layer 2 multicast packets received on the interface. This is a subset of the total output packet count.

Related Commands

Command	Description
interface bvi , on page 66	

Layer 2 Access List Commands

This section describes the commands used to configure Layer 2 access list.

For detailed information about concepts and configuration, see the Configure Layer 2 Access Control Lists chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco 8000 Series Routers*.

ethernet-services access-group

To control access to an interface, use the **ethernet-service access-group** command in interface configuration mode.

ethernet-services access-group *access-list-name* **ingress**

Syntax Description

access-list-name	Name of an Ethernet services access list as specified by the **ethernet-service access-list** command.
ingress	Filters on inbound packets.

Command Default

The interface does not have an Ethernet services access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

The **ethernet-services access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *access-list-name* argument to specify a particular Ethernet services access list. Use the ingress keyword to filter on inbound packets.

If the list permits the addresses, the software continues to process the packet. If the access list denies the address, the software discards the packet.

If the specified access list does not exist, all packets are passed.

By default, the unique or per-interface ACL statistics are disabled.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to apply filters on inbound packets from an interface.

```
Router# configure
Router(config)# interface HundredGigE 0/0/0/24
Router(config-if)# l2transport
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

ethernet-services access-list

To define an Ethernet services (Layer 2) access list by name, use the **ethernet-services access-list** command in global configuration mode.

ethernet-services access-list *access-list-name*

Syntax Description

access-list-name	Name of the Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.

Command Default

No Ethernet services access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

The **ethernet-services access-list** command places the router in access list configuration mode, in which the denied or permitted access conditions must be defined.

Layer 2 access control lists are supported only for the field's L2 source and destination address, EtherType, Outer VLAN ID, Inner VLAN ID, Class of Service (COS), and VLAN DEI.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to configure ethernet-services access-list:

```
Router# configure
Router(config)# ethernet-services access-list es_acl_1
Router(config-es-acl)# 10 deny 00ff.eedd.0010 ff00.0000.00ff 0000.0100.0001 0000.0000.ffff
Router(config-es-acl)# 20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
Router(config-es-acl)# 30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
Router(config-es-acl)# commit
Router(config)# interface HundredGigE 0/0/0/24
Router(config-if)# l2transport
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

show access-lists ethernet-services

To display the contents of current Ethernet services access lists, use the **show access-lists ethernet-services** command in EXEC mode.

show access-lists ethernet-services *access-list-name* [**hardware**] **ingress** [**detail**] [**location** { *location* | **all** }]

Syntax Description

access-list-name	Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
hardware	(Optional) Display Ethernet services access list entries in hardware including the match count for a specific ACL in a particular direction across the line card.
ingress	Filters on inbound packets.
detail	(Optional) Display TCAM entries.
location	(Optional) Display information for a specific node number.
location	Fully qualified location specification.
all	Displays packet filtering usage for all interface cards.

Command Default

The contents of all Ethernet services access lists are displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows sample output for the **show access-lists ethernet-services** command:

```
Router# show access-lists ethernet-services es_acl_1 hardware ingress location 0/0/CPU0
Thu Nov  3 22:02:27.222 UTC
ethernet-services access-list es_acl_1
 10 deny any host fcd7.844c.7486 cos 3   (65334 matches)
 20 deny any host fcd7.844c.7486
 30 permit any any
```

```
Router# show access-lists ethernet-services es_acl_1 hardware ingress detail location
0/0/CPU0
```

```
Thu Nov  3 22:01:18.620 UTC
es_acl_1 Details:
Sequence Number: 10
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: FCD7:844C:7486
 Destination MAC Mask: FFFF:FFFF:FFFF
COS: 0x03
        Entry Index: 0x0
        DPA Handle: 0x89BF60E8

es_acl_1 Details:
Sequence Number: 20
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: FCD7:844C:7486
 Destination MAC Mask: FFFF:FFFF:FFFF
        Entry Index: 0x0
        DPA Handle: 0x89BF62E8

es_acl_1 Details:
Sequence Number: 30
Number of DPA Entries: 1
ACL ID: 1
ACE Action: PERMIT
ACE Logging: DISABLED
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: 0000:0000:0000
 Destination MAC Mask: 0000:0000:0000
        Entry Index: 0x0
        DPA Handle: 0x89BF64E8

es_acl_1 Details:
Sequence Number: IMPLICIT DENY
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: 0000:0000:0000
 Destination MAC Mask: 0000:0000:0000
        Entry Index: 0x0
        DPA Handle: 0x89BF66E8
```

show access-lists ethernet-services usage pfilter

To identify the modes and interfaces on which a particular access-list is applied, use the **show access-lists ethernet-services usage pfilter** command in EXEC mode. Information displayed includes the application of all or specific access-lists, the interfaces on which they have been applied and the direction in which they are applied.

show access-lists ethernet-services *access-list-name* **usage pfilter location** { *location* | **all** }

Syntax Description

access-list-name	Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
usage	Displays the usage of the Ethernet services access list on a given interface card
pfilter	Displays the packet filtering usage for the specified interface card.
location	Interface card on which the access list information is needed.
location	Fully qualified location specification.
all	Displays packet filtering usage for all interface cards.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to display packet filter usage at a specific location:

```
Router# show access-lists ethernet-services es_acl_1 usage pfilter location 0/0/CPU0
Interface : HundredGigE 0/0/0/24
    Input ACL : es_acl_1
    Output ACL : N/A
```