Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Command Reference, Release 4.2.x

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

Text Part Number: OL-26119-02

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

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

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

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

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

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

CONTENTS

Preface

CHAPTER 1

CHAPTER 2

Preface

The *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Command Reference* preface contains these sections:

Changes to This Document

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

Revision	Date	Change Summary
OL-26119-02	June 2012	Republished with documentation updates for Cisco IOS XR Release 4.2.1
OL-26119-01	December 2011	Initial release of this document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Ethernet Interfaces Commands

This module describes the Cisco IOS XR software commands used to configure the Ethernet interfaces on the Cisco ASR 9000 Series Router.

Note This module does not include the commands for Management Ethernet interfaces and Ethernet OAM. To configure a Management Ethernet interface for routing or modify the configuration of a Management Ethernet interface or to configure Ethernet OAM, use the commands described in the *Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*

Refer to the *Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Command Reference* for more information on the Ethernet Interfaces and Ethernet OAM commands.

dot1q tunneling ethertype

To configure the Ethertype, used by peer devices when implementing QinQ VLAN tagging, to be 0x9100, use the **dot1q tunneling ethertype** command in the interface configuration mode for an Ethernet interface. To return to the default Ethertype configuration (0x8100), use the **no** form of this command.

dot1q tunneling ethertype {**0x9100**| **0x9200**}

no dot1q tunneling ethertype

Syntax Description

0x9100	Sets the Ethertype value to 0x9100.
0x9200	Sets the Ethertype value to 0x9200.

Command Default

The Ethertype field used by peer devices when implementing QinQ VLAN tagging is either 0x8100 or 0x8200.

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

The **dot1q tunneling ethertype** command can be applied to a main interface. When applied to the main interface, it changes the subinterfaces, that have been configured with an **encapsulation dot1q second-dot1q** command, under that main interface.

This command changes the outer VLAN tag from 802.1q Ethertype 0x8100 to 0x9100 or 0x9200.

Task ID

Task ID	Operations
vlan	read, write

Examples

The following example shows how to configure the Ethertype to 0x9100:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
```

```
RP/0/RSP0/CPU0:router(config-if)# dot1q tunneling ethertype 0x9100
RP/0/RSP0/CPU0:router(config-if)#
```

The following example shows how to configure the Ethertype to 0x9200:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/1
RP/0/RSP0/CPU0:router(config-if)# dot1q tunneling ethertype 0x9200
RP/0/RSP0/CPU0:router(config-if)#
```

Related Commands

Command	Description
encapsulation dot1q, on page 8	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1ad dot1q, on page 6	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 10	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation untagged, on page 12	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

encapsulation default

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

encapsulation default

no encapsulation default

Syntax Description

This command has no keywords or arguments.

Command Default

No default service instance is configured on the port.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

Only one encapsulation command must be configured per service instance.

Examples

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

```
RP/0/RSP0/CPU0:router(config-if)# encapsulation default
```

Related Commands

Command	Description
encapsulation dot1q, on page 8	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

Command	Description
encapsulation dot1ad dot1q, on page 6	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 10	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation untagged, on page 12	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

encapsulation dot1ad dot1q

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

encapsulation dot1ad *vlan-id* **dot1q** *vlan-id*

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

Syntax Description

dot1ad	Indicates that the IEEE 802.1ad provider bridges encapsulation type is used for the outer tag.
dot1q	Indicates that the IEEE 802.1q standard encapsulation type is used for the inner tag.
vlan-id	VLAN ID, integer in the range 1 to 4094. A hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) A comma must be entered to separate each VLAN ID range from the next range.

Command Default

No matching criteria are defined.

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

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

Some of the fields in the 802.1ad VLAN header are interpreted differently per 802.1ad standard. A **tunneling ethertype** command applied to the main interface does not apply to an 802.1ad subinterface.

An interface with encapsulation dot1ad causes the router to categorize the interface as an 802.1ad interface. This causes special processing for certain protocols and other features:

- MSTP uses the IEEE 802.1ad MAC STP address instead of the STP MAC address.

- Certain QoS functions may use the Drop Eligibility (DE) bit of the IEEE 802.1ad tag.

Examples

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

```
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1ad 100 dot1q 20
```

Related Commands

Command	Description
encapsulation default, on page 4	Configure the default service instance on a port.
encapsulation dot1q, on page 8	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation untagged, on page 12	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

encapsulation dot1q

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

encapsulation dot1q *vlan-id* [,*vlan-id* [*-vlan-id*]] [**exact**| **ingress source-mac** *mac-address*| **second-dot1q** *vlan-id*]

encapsulation dot1q *vlan-id,* **untagged**

no encapsulation dot1q

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) Comma must be entered to separate each VLAN ID range from the next range.
exact	(Optional) Prevents matching of frames with more than one tag.
ingress source-mac	(Optional) Performs MAC-based matching.
untagged	(Optional) Allows matches for both the single-tag dot1q frames and untagged frames.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.1	The **ingress source-mac** keyword was added.
Release 4.0.1	This command was supported on l2transport subinterfaces.

Usage Guidelines

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

Only one encapsulation statement can be applied to a subinterface. Encapsulation statements cannot be applied to main interfaces.

A single encapsulation dot1q statement specifies matching for frames with a single VLAN ID; a range of VLAN IDs; or a single VLAN ID or untagged.

Examples

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

```
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 10
```

The following example shows how to map 802.1Q frames ingress on an l2transport subinterface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/3.10 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 10
```

Related Commands

Command	Description
encapsulation default, on page 4	Configure the default service instance on a port.
encapsulation dot1ad dot1q, on page 6	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 10	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation untagged, on page 12	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

encapsulation dot1q second-dot1q

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

encapsulation dot1q *vlan-id* **second-dot1q** {**any**| *vlan-id* [,*vlan-id [-vlan-id]*]} [**exact**| **ingress source-mac** *mac-address*]

no encapsulation dot1q *vlan-id* **second-dot1q** {**any**| *vlan-id* [,*vlan-id [-vlan-id]*]} [**exact**| **ingress source-mac** *mac-address*]

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094. A hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) A comma must be entered to separate each VLAN ID range from the next range.
second-dot1q	(Optional) Specifies IEEE 802.1Q VLAN tagged packets.
any	Any second tag in the range 1 to 4094.
exact	(Optional) Ensures that frames with more than two tags do not match.
ingress source-mac	(Optional) Performs MAC-based matching.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.1	The **ingress source-mac** keyword was added.

Usage Guidelines

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

The criteria for this command are: the outer tag must be unique and the inner tag may be a single VLAN, a range of VLANs or lists of the previous two.

QinQ service instance, allows single, multiple or range on second-dot1q.

Only one encapsulation command must be configured per service instance.

Examples

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

```
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q second-dot1q 20
```

Related Commands

Command	Description
encapsulation default, on page 4	Configure the default service instance on a port.
encapsulation dot1ad dot1q, on page 6	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q, on page 8	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation untagged, on page 12	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

encapsulation untagged

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

encapsulation untagged [**ingress source-mac** *mac-address*]

no encapsulation untagged

Syntax Description

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

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.1	The **ingress source-mac** keyword was added.

Usage Guidelines

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

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

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

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

Examples

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

Example 1:

```
RP/0/RSP0/CPU0:router(config-if)# encapsulation untagged
```

Example 2:

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/1/0.100 l2transport
RP/0/RSP0/CPU0:router(config-subif)# encapsulation untagged
```

Related Commands

Command	Description
encapsulation default, on page 4	Configure the default service instance on a port.
encapsulation dot1q, on page 8	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 10	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.

ethernet egress-filter

To enable strict egress filtering on all subinterfaces on the router by default, use the **ethernet egress-filter** command in global configuration mode.

ethernet egress-filter strict

To enable or disable egress filtering explicitly on any Layer 2 subinterface, use the **ethernet egress-filter** command in Layer 2 subinterface mode.

ethernet egress-filter {**strict**| **disabled**}

Syntax Description

strict	Enables strict egress EFP filtering on the interface. Only packets that pass the ingress EFP filter on the interface can be transmitted out of this interface. Other packets are dropped at the egress filter.
disabled	Disables strict egress EFP filtering on the interface. This allows packets that do not match the interface encapsulation to be transmitted out of the interface.

Command Default

For platforms that support this command, the global default is that subinterface egress encapsulation filtering is disabled.

Command Modes

Global configuration and Layer 2 subinterface configuration

Command History

Release	Modification
Release 3.7.3	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enable strict egress filtering on all subinterfaces in global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet egress-filter strict
```

The following example shows how to enable the strict egress filtering on any Layer 2 subinterface in Layer 2 subinterface mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/1.1
RP/0/RSP0/CPU0:router(config-subif)# ethernet egress-filter strict
```

ethernet filtering

To enable ethernet filtering on interfaces on the router, use the **ethernet filtering** command in the interface configuration mode. To disable ethernet filtering, use the **no** form of the command.

ethernet filtering {**dot1ad**| **dot1q**}

no ethernet filtering

Syntax Description

dot1ad	Filters only the Ethernet multicast protocol addresses that are reserved by IEEE 802.1ad, used for C-facing interfaces, to prevent C-network traffic from interfering with the S-network protocols.
dot1q	Filters all Ethernet multicast protocol addresses.

Command Default

Ethernet filtering is not enabled.

Command Modes

interface configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

The following table lists the DA MAC addresses and specifies the action taken when either the dot1q or the dot1ad keywords are used:

DA MAC Address	Description	dot1q	dot1ad
01-80-C2-00-00-00	STP, RSTP, MSTP, etc.	Discard	Data
01-80-C2-00-00-01	802.3X Pause Protocol	Discard	Discard
01-80-C2-00-00-02	Slow Protocols: 802.3ad LACP, 802.3ah OAM	Discard	Discard
01-80-C2-00-00-03	802.1X	Discard	Discard
01-80-C2-00-00-04	Reserved	Discard	Discard

DA MAC Address	Description	dot1q	dot1ad
01-80-C2-00-00-05	Reserved	Discard	Discard
01-80-C2-00-00-06	Reserved	Discard	Discard
01-80-C2-00-00-07	Reserved	Discard	Discard
01-80-C2-00-00-08	Provider Bridge Group Address (e.g. MSTP BPDU)	Discard	Discard
01-80-C2-00-00-09	Reserved	Discard	Discard
01-80-C2-00-00-0A	Reserved	Discard	Discard
01-80-C2-00-00-0B	Reserved	Discard	Data
01-80-C2-00-00-0C	Reserved	Discard	Data
01-80-C2-00-00-0D	Provider Bridge GVRP address	Discard	Data
01-80-C2-00-00-0E	802.1ab-LLDP	Discard	Data
01-80-C2-00-00-0F	Reserved	Discard	Data
01-80-C2-00-00-10	All Bridges address	Discard	Data
01-80-C2-00-00-20	GMRP / MMRP	Discard	Data
01-80-C2-00-00-21	GVRP / MVRP	Discard	Data
01-80-C2-00-00-22-2F	Other GARP addresses	Discard	Data
01-00-0C-CC-CC-CC	CDP, DTP, VTP, PaGP, UDLD	Discard	Data

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to apply ethernet filtering on a main interface:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#interface GigabitEthernet0/5/0/1
RP/0/RSP0/CPU0:router(config-if)#ethernet filtering dot1q
```

```
RP/0/RSP0/CPU0:router(config-if)#l2transport
RP/0/RSP0/CPU0:router(config-if-l2)#commit

RP/0/RSP0/CPU0:router#show run | begin GigabitEthernet0/5/0/1
Tue Nov 24 12:29:55.718 EST
Building configuration...
interface GigabitEthernet0/5/0/1
 mtu 1500
 ethernet filtering dot1q
 l2transport
 !
!
interface GigabitEthernet0/5/0/2
 shutdown
!
interface GigabitEthernet0/5/0/3
 shutdown
!
interface GigabitEthernet0/5/0/4
 shutdown
!
interface GigabitEthernet0/5/0/5
 shutdown
!
interface GigabitEthernet0/5/0/6
 shutdown
!
interface GigabitEthernet0/5/0/7
 shutdown
RP/0/RSP0/CPU0:router#
```

The following example shows how to apply ethernet filtering on a subinterface:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#interface GigabitEthernet0/5/0/1
RP/0/RSP0/CPU0:router(config-if)#ethernet filtering dot1q
RP/0/RSP0/CPU0:router(config-if)#interface GigabitEthernet0/5/0/1.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)#encapsulation untagged
RP/0/RSP0/CPU0:router(config-subif)#commit
RP/0/RSP0/CPU0:router(config-subif)#end

RP/0/RSP0/CPU0:router#show run | begin GigabitEthernet0/5/0/1
Tue Nov 24 12:26:25.494 EST
Building configuration...
interface GigabitEthernet0/5/0/1
 mtu 1500
 ethernet filtering dot1q
!
interface GigabitEthernet0/5/0/1.1 l2transport
 encapsulation untagged
!
interface GigabitEthernet0/5/0/2
 shutdown
!
interface GigabitEthernet0/5/0/3
 shutdown
!
interface GigabitEthernet0/5/0/4
 shutdown
!
interface GigabitEthernet0/5/0/5
 shutdown
!
interface GigabitEthernet0/5/0/6
 shutdown
!
interface GigabitEthernet0/5/0/7
RP/0/RSP0/CPU0:router#
```

Note Ethernet filtering is configured on the main interface; however, the configuration affects the subinterface and not the main interface.

ethernet source bypass egress-filter

To mark all ingress packets, received on the interface, to indicate that the packets should bypass any strict egress filter on any egress interface, use the **ethernet source bypass egress-filter** command in the subinterface configuration mode. To allow packets without being marked, use the **no** form of this command.

ethernet source bypass egress-filter

no ethernet source bypass egress-filter

This command has no keywords or arguments.

Command Default

None

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to mark all ingress packets received on the interface:

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet0/0/0/0/3.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 1
RP/0/RSP0/CPU0:router(config-subif)# rewrite ingress tag translate 1-to-1 dot1q 4094 symmetric
RP/0/RSP0/CPU0:router(config-subif)# ethernet egress-filter disabled
RP/0/RSP0/CPU0:router(config-subif)# ethernet source-bypass-egress-filter
```

Related Commands

Command	Description
encapsulation dot1q, on page 8	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

l2protocol (Ethernet)

To configure Layer 2 protocol tunneling and protocol data unit (PDU) filtering on an Ethernet interface, use the **l2protocol** command in Layer 2 transport configuration mode. To disable a Layer 2 protocol tunneling and Layer 2 protocol data units configuration, use the **no** form of this command.

l2protocol cpsv {**tunnel**| **reverse-tunnel**}

no l2protocol

Syntax Description

cpsv	Enables L2PT for the interface. L2PT is enabled for the following protocols only: • CDP • STP • VTP **Note** STP includes all Spanning Tree protocol derivatives (RSTP, MSTP, etc.)
tunnel	Performs L2PT encapsulation on frames as they enter the interface. Also, performs L2PT de-encapsulation on frames as they exit they interface. L2PT encapsulation rewrites the destination MAC address with the L2PT destination MAC address. L2PT deencapsulation replaces the L2PT destination MAC address with the original destination MAC address.
reverse-tunnel	Performs L2PT encapsulation on frames as they exit the interface. Also, perform L2PT deencapsulation on frames as they enter the interface.

Command Default

All Layer 2 protocol data units are forwarded through the network without modification.

Command Modes

Layer 2 transport configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Note The **l2protocol** command is available only when Layer 2 transport port mode is enabled on the interface with the **l2transport** command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure an Ethernet interface to tunnel in the ingress direction:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/0/0/1
RP/0/RSP0/CPU0:router(config-if)# l2transport
RP/0/RSP0/CPU0:router(config-if-l2)# l2protocol cpsv tunnel
```

Related Commands

Command	Description
l2transport (Ethernet), on page 23	Enables Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode.

l2transport (Ethernet)

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

l2transport

no l2transport

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

When you issue the **l2transport** command in interface configuration mode, the CLI prompt changes to "config-if-l2," indicating that you have entered the Layer 2 transport configuration submode. In the following sample output, the question mark (**?**) online help function displays all the commands available under Layer 2 transport configuration submode for an Ethernet interface:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
RP/0/RSP0/CPU0:router(config-if)# l2transport
RP/0/RSP0/CPU0:router(config-if-l2)# ?
  commit          Commit the configuration changes to running
  describe        Describe a command without taking real actions
  do              Run an exec command
  exit            Exit from this submode
  no              Negate a command or set its defaults
  service-policy  Configure QoS Service policy
  show            Show contents of configuration
RP/0/RSP0/CPU0:router(config-if-l2)#
```

Note The **l2transport** command is mutually exclusive with any Layer 3 interface configuration.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEther 0/2/0/0
RP/0/RSP0/CPU0:router(config-if)# l2transport
RP/0/RSP0/CPU0:router(config-if-l2)#
```

The following example shows how to use the **l2transport** keyword in the **interface** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEther 0/2/0/0 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 200
RP/0/RSP0/CPU0:router(config-if-l2)#commit
```

The following example shows how to use the **l2transport** command on an Ethernet subinterface:

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

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#interface GigabitEthernet 0/5/0/1.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)#encapsulation dot1q 100
RP/0/RSP0/CPU0:router(config-subif)#ethernet egress-filter strict
RP/0/RSP0/CPU0:router(config-subif)#commit
RP/0/RSP0/CPU0:router(config-subif)#end

RP/0/RSP0/CPU0:router#sh run | begin GigabitEthernet0/5/0/1
Thu Dec  3 10:15:40.916 EST Building configuration...
interface GigabitEthernet0/5/0/1
 mtu 1500
 ethernet filtering dot1q
!
interface GigabitEthernet0/5/0/1.1 l2transport
encapsulation dot1q 100
ethernet egress-filter strict !
interface GigabitEthernet0/5/0/2
 shutdown
!
!
```

Note To configure l2transport on an Ethernet subinterface, ensure that the main interface is configured as a Layer 3 interface.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or for a specific node.
show l2vpn xconnect	Displays brief information on configured xconnects.

local-traffic default encapsulation

To enable Connectivity Fault Management (CFM) to identify a range of VLAN IDs that are to be used as the default for sourcing CFM packets from the interface, use the **local-traffic default encapsulation** command in the subinterface configuration mode. To return to the default behavior, use the **no** form of this command.

local-traffic default encapsulation {**dot1q** *vlan-id*| **dot1q** *vlan-id* **second-dot1q** *vlan-id*| **dot1ad** *vlan-id*| **dot1ad** *vlan-id* **dot1q** *vlan-id*}

no local-traffic default encapsulation {**dot1q** *vlan-id*| **dot1q** *vlan-id* **second-dot1q** *vlan-id*| **dot1ad** *vlan-id*| **dot1ad** *vlan-id* **dot1q** *vlan-id*}

Syntax Description

dot1q	Indicates that the IEEE 802.1q standard encapsulation type is used.
second-dot1q	Indicates that the IEEE 802.1q encapsulation is used.
dot1ad	Indicates that the IEEE 802.1ad provider bridges encapsulation type is used.
vlan-id	Specifies the VLAN ID as an integer. The range is 1 to 4094. A hyphen separates the starting and ending VLAN ID values that are used when defining a range of VLAN IDs.

Command Default

Lowest numbered VLAN ID is chosen.

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

The tag stack configured by the **local-traffic default encapsulation** command must match the encapsulation specified for this interface in the **encapsulation** command.

For packets that are sent as responses to incoming packets, the encapsulation that is to be used may be derived from the incoming packet. This command determines the encapsulation to use when this is not the case.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example indicates that the locally sourced frames (not sent in response to another ingress frame) sent out of GigabitEthernet subinterface 0/3/0/1.1 should be tagged with 802.1Q VLAN 50. When the local-traffic is not configured, chooses the lowest value in the range and sends the frames out tagged with 802.1Q VLAN 10.

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/3/0/1.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 10-100
RP/0/RSP0/CPU0:router(config-subif)# local-traffic default encapsulation dot1q 50
```

The followoing example indicates that the locally sourced frames are sent out with an outer VLAN tag of 802.1Q 1000, and an inner VLAN tag of 802.1Q 500. Without configuring the local-traffic, the frames are sent out with an outer VLAN tag of 1000 and an inner VLAN tag of 1:

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet0/0/0/0.2 l2transport
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 1000 second-dot1q 1-500
RP/0/RSP0/CPU0:routerr(config-subif)# local-traffic default encapsulation dot1q 1000
second-dot1q 500
```

rewrite ingress tag

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

rewrite ingress tag {**push** {**dot1q** *vlan-id*| **dot1q** *vlan-id* **second-dot1q** *vlan-id*| **dot1ad** *vlan-id* **dot1q** *vlan-id*}| **pop** {**1**| **2**}| **translate** {**1to1** {**dot1q** *vlan-id*| **dot1ad** *vlan-id*}| **2-to-1** **dot1q** *vlan-id*| **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id*| **dot1ad** *vlan-id* **dot1q** *vlan-id*}| **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id*| **dot1ad** *vlan-id* **dot1q** *vlan-id*}} **[symmetric]**

no rewrite ingress tag {**push** {**dot1q** *vlan-id*| **dot1q** *vlan-id* **second-dot1q** *vlan-id*| **dot1ad** *vlan-id* **dot1q** *vlan-id*}| **pop** {**1**| **2**}| **translate** {**1to1** {**dot1q** *vlan-id*| **dot1ad** *vlan-id*}| **2-to-1** **dot1q** *vlan-id*| **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id*| **dot1ad** *vlan-id* **dot1q** *vlan-id*}| **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id*| **dot1ad** *vlan-id* **dot1q** *vlan-id*}} **[symmetric]**

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094.
push dot1q *vlan-id*	Pushes one 802.1Q tag with *vlan-id*.
push dot1q *vlan-id* **second-dot1q** *vlan-id*	Pushes a pair of 802.1Q tags in the order first, second.
pop {1 | 2}	One or two tags are removed from the packet. This command can be combined with a push (pop N and subsequent push *vlan-id*).
translate 1-to-1 dot1q *vlan-id*	Replaces the incoming tag (defined in the encapsulation command) into a different 802.1Q tag at the ingress service instance.
translate 2-to-1 dot1q *vlan-id*	Replaces a pair of tags defined in the **encapsulation** command by vlan-id.
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.

Command Default

The frame is left intact on ingress.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

The **pop** command assumes the elements being popped are defined by the encapsulation type. The exception case should be drop the packet.

The **rewrite ingress tag translate**command assume the tags being translated from are defined by the encapsulation type. In the 2-to-1 option, the “2” means “2 tags of a type defined by the **encapsulation** command. The translation operation requires at least “from” tag in the original packet. If the original packet contains more tags than the ones defined in the “from”, then the operation should be done beginning on the outer tag. Exception cases should be dropped.

Examples

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

```
RP/0/RSP0/CPU0:router(config-if)# rewrite ingress push dot1q 200
```

Related Commands

Command	Description
encapsulation default, on page 4	Configure the default service instance on a port.
encapsulation dot1ad dot1q, on page 6	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q, on page 8	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 10	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation untagged, on page 12	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

Generic Routing Encapsulation Commands

This module describes the commands used to configure generic routing encapsulation (GRE).

For detailed information about GRE concepts, configuration tasks, and examples, refer to the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

bandwidth

To set the tunnel interface bandwidth, use the **bandwidth** command in interface configuration mode. To undo the tunnel interface bandwidth that is set, use the **no** form of this command.

bandwidth *kbps*

no bandwidth *kbps*

Syntax Description

kbps	Interface bandwidth in kilobits per second (kbps). The range is from 0 to 4294967295. The default value is 100.

Command Default

None

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
interface	read, write

Examples

This example shows how to set the bandwidth of the tunnel interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 6677
RP/0/RSP0/CPU0:router(config-if)# bandwidth 56789
```

description (GRE)

To specify the description of any interface, use the **description** command in the interface configuration mode. To undo the specified description, use the **no** form of the command.

description *description-name*

no description

Syntax Description

description-name	Description of the Interface.

Command Default

None

Command Modes

Interface Configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
interface	read, write

Examples

The following output shows how to specify the description of an interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 789
RP/0/RSP0/CPU0:router(config-if)# description Interface
```

ipv4 address

To set the IPv4 address of the tunnel interface, use the **ipv4 address** command in interface configuration mode. To remove the IPv4 addresses, use the **no** form of this command.

ipv4 address *prefix subnet mask* [**route-tag** *value*| **secondary** [**route-tag** *value*]]

no ipv4 address *prefix subnet mask* [**route-tag** *value*| **secondary** [**route-tag** *value*]]

Syntax Description

prefix	IPv4 address of the interface.
subnet mask	Subnet mask of the interface.
route-tag	Specifies the tag associated with the IP address.
value	Tag value.
secondary	Specifies the secondary IPV4 address.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read, write
acl	read, write

Examples

This example shows how to set the IPV4 address with route-tag option:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface tunnel-ip 67 ipv4 address 10.1.1.2 6.7.7.8
route-tag 78
```

This example shows how to set the IPV4 address with secondary option:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface tunnel-ip 67 ipv4 address 1.2.3.4 7.8.9.8
secondary route-tag 89
```

ipv4 mtu (LxVPN)

To set the IPv4 MTU on the tunnel interface, use the **ipv4 mtu** command in interface configuration mode. To remove the IPv4 MTU, use the **no** form of this command.

ipv4 mtu *size*

no ipv4 mtu *size*

Syntax Description

size	Size of the MTU in bytes. The range is from 68 to 65535.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read, write
acl	read, write

Examples

This example shows how to set the IPv4 MTU:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface tunnel-ip 78 ipv4 mtu 78
```

ipv6 address (LxVPN)

To set the IPv6 address of the tunnel interface, use the **ipv6 address** command in interface configuration mode. To remove the IPv6 addresses, use the **no** form of this command.

ipv6 {**address zone** {**prefix length**| **link-local**} [**route-tag** *value*]| **zone**/**length** [**route-tag value**]}

no ipv6 {**address zone** {**prefix length**| **link-local**} [**route-tag** *value*]| **zone**/**length** [**route-tag value**]}

Syntax Description

zone	Specifies the IPv6 address of the interface.
prefix length	Specifies the length of the IPv6 address prefix, in bits. The range is from 1 to 128.
link-local	Specifies the link-local address.
route-tag	Specifies the tag associated with the address.
value	Tag value. The range is from 1 to 4294967295.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read, write
interface	read, write
ipv6	read, write

Examples

This example shows how to set the ipv6 address for a tunnel interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface tunnel-ip 67 ipv6 address 10:2::3 link-local
route-tag 78
```

ipv6 mtu (LxVPN)

To set the IPv6 MTU on the tunnel interface, use the **ipv6 mtu** command in interface configuration mode. To remove the IPv6 MTU, use the **no** form of this command.

ipv6 mtu *size*

no ipv6 mtu *size*

Syntax Description

size	Size of the MTU in bytes. The range is from 1280 to 65535.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read, write
interface	read, write
ipv6	read, write

Examples

This example shows how to set the IPv4 MTU:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface tunnel-ip 78 ipv6 mtu 3456
```

keepalive

To enable keepalive for a tunnel interface, use the **keepalive** command. To remove keepalive, use the **no** form of this command.

keepalive [*time_in_seconds* [*retry_num*]]

no keepalive

Syntax Description

time_in_seconds	Specifies the frequency (in seconds) at which keepalive check is performed. The default is 10 seconds. The minimum value is 1 second.
retry_num	Specifies the number of keepalive retries before declaring that a tunnel destination is unreachable. The default is 3 retries. The minimum value is 1 retry.

Command Default

None

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **keepalive** command to enable keepalive for a tunnel interface.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RSP0/CPU0:router(config-if)# keepalive 30
```

mtu (GRE)

To set the MTU size of the tunnel interface, use the **mtu** command in interface configuration mode. To undo the MTU size of the tunnel interface that is set, use the **no** form of this command.

This is a Generic Routing Encapsulation (GRE) command.

mtu *size*

no mtu *size*

Syntax Description

size	Size of MTU in bytes. The default value is 1476.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
interface	read, write

Examples

This example shows how to set the MTU size of the tunnel interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 456
RP/0/RSP0/CPU0:router(config-if)# mtu 334
```

shutdown (GRE)

To shut down any interface, use the **shutdown** command in interface configuration mode. To start the interface, use the **no** form of the command.

This is a Generic Routing Encapsulation (GRE) command.

shutdown

no shutdown

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
interface	read, write

Examples

This example shows how to shut down a given interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 789
RP/0/RSP0/CPU0:router(config-if)# shutdown
```

tunnel destination

To specify a tunnel interface's destination, use the **tunnel destination** command. To remove the destination, use the **no** form of this command.

Note The tunnel will not be operational until the tunnel destination is specified.

tunnel destination *A.B.C.D*

no tunnel destination *A.B.C.D*

Syntax Description

A.B.C.D	Specifies the IPv4 address of the host destination.

Command Default

None

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RSP0/CPU0:router(config-if)# tunnel destination 10.10.10.1
```

Related Commands

Command	Description
tunnel mode, on page 47	Sets the encapsulation mode of the tunnel interface.
tunnel source, on page 49	Sets a tunnel interface's source address.
tunnel tos, on page 51	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 53	Configures the Time-To-Live (TTL) for packets entering the tunnel.

tunnel dfbit disable

To configure the DF bit setting in the tunnel transport header, use the **tunnel dfbit disable** command. To revert to the default DF bit setting value, use the **no** form of this command.

tunnel dfbit disable

no tunnel dfbit disable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **tunnel dfbit disable** command specifies the DF bit setting in the tunnel transport header. The default is to always set the DF bit. Hence, use the **tunnel dfbit disable** command to override the default.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RSP0/CPU0:router(config-if)# tunnel dfbit disable
```

Related Commands

Command	Description
tunnel destination, on page 43	Specifies a tunnel interface's destination.
tunnel mode, on page 47	Sets the encapsulation mode of the tunnel interface.

Command	Description
tunnel source, on page 49	Sets a tunnel interface's source address.
tunnel tos, on page 51	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 53	Configures the Time-To-Live (TTL) for packets entering the tunnel.

tunnel mode

To set the encapsulation mode of the tunnel interface, use the **tunnel mode** command. To remove the encapsulation mode, use the **no** form of this command.

Note The tunnel will not be operational until the encapsulation mode is specified. Only one mode can be specified for a tunnel instance at any given time.

tunnel mode gre ipv4

no tunnel mode

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RSP0/CPU0:router(config-if)#tunnel mode gre ipv4
```

Related Commands

Command	Description
tunnel destination, on page 43	Specifies a tunnel interface's destination.
tunnel source, on page 49	Sets a tunnel interface's source address.
tunnel tos, on page 51	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 53	Configures the Time-To-Live (TTL) for packets entering the tunnel.

tunnel source

To set a tunnel interface's source address, use the **tunnel source** command. To remove the source address, use the **no** form of this command.

Note The tunnel will not be operational until the tunnel source is specified.

tunnel source {**interface_name**| **A.B.C.D**}

no tunnel source {**interface_name**| **A.B.C.D**}

Syntax Description

interface_name	Specifies the name of the interface whose IP address will be used as the source address of the tunnel. The interface name can be of a loopback interface or a physical interface.
A.B.C.D	Specifies the IPv4 address to use as the source address for packets in the tunnel.

Command Default

None

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RSP0/CPU0:router(config-if)# tunnel source 10.10.10.1
```

Related Commands

Command	Description
tunnel destination, on page 43	Specifies a tunnel interface's destination.
tunnel mode, on page 47	Sets the encapsulation mode of the tunnel interface.
tunnel tos, on page 51	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 53	Configures the Time-To-Live (TTL) for packets entering the tunnel.

tunnel tos

To specify the value of the TOS field in the tunnel encapsulating packets, use the **tunnel tos** command. To return to the default TOS value, use the **no** form of this command.

tunnel tos *tos_value*

no tunnel tos *tos_value*

Syntax Description

tos_value	Specifies the value of the TOS field in the tunnel encapsulating packets. The TOS value ranges between 0 to 255.

Command Default

Copies the TOS/COS bits of the internal IP header to the GRE IP header. In case of labeled payload, EXP bits are copied to TOS bits of the GRE IP header.

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RSP0/CPU0:router(config-if)# tunnel tos 100
```

Related Commands

Command	Description
tunnel destination, on page 43	Specifies a tunnel interface's destination.

Command	Description
tunnel mode, on page 47	Sets the encapsulation mode of the tunnel interface.
tunnel source, on page 49	Sets a tunnel interface's source address.
tunnel ttl, on page 53	Configures the Time-To-Live (TTL) for packets entering the tunnel.

tunnel ttl

To configure the Time-To-Live (TTL) for packets entering the tunnel, use the **tunnel ttl** command. To undo the configuration, use the **no** form of this command.

tunnel ttl *ttl_value*

no tunnel ttl *ttl_value*

Syntax Description

ttl_value	Specifies the value of TTL for packets entering the tunnel. The TTL value ranges between 1 to 255.

Command Default

The default TTL value is set to 255.

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

This command specifies the Time-To-Live for packets entering the tunnel so that the packets are not dropped inside the carrier network before reaching the tunnel destination.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RSP0/CPU0:router(config-if)#tunnel source 10.10.10.1
```

Related Commands

Command	Description
tunnel destination, on page 43	Specifies a tunnel interface's destination.
tunnel mode, on page 47	Sets the encapsulation mode of the tunnel interface.
tunnel tos, on page 51	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel source, on page 49	Sets a tunnel interface's source address.

Point to Point Layer 2 Services Commands

This module describes the commands used to configure, monitor, and troubleshoot a Layer 2 or Layer 3 virtual private network (VPN).

For detailed information about virtual private network concepts, configuration tasks, and examples, refer to the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

backup (L2VPN)

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

backup neighbor *IP-address* **pw-id** *value*

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN xconnect p2p pseudowire configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure backup pseudowires:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group gr1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p p001
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# neighbor 10.1.1.1 pw-id 2
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)#
```

Related Commands

Command	Description
backup disable (L2VPN), on page 59	Specifies how long a backup pseudowire should wait before resuming operation after the primary pseudowire goes down.
l2vpn, on page 83	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 95	Configures a pseudowire for a cross-connect.
p2p, on page 106	Enters p2p configuration submode to configure point-to-point cross-connects.
xconnect group, on page 136	Configures cross-connect groups.

backup disable (L2VPN)

To specify how long a backup pseudowire should wait before resuming primary pseudowire operation after the failure with primary pseudowire has been cleared, use the **backup disable** command in L2VPN pseudowire class configuration mode. To disable this feature, use the **no** form of this command.

backup disable {**delay** *value*| **never**}

no backup disable {**delay** *value*| **never**}

Syntax Description

delay *value*	Specifies the number of seconds that elapse after the failure with primary pseudowire has been cleared before the Cisco IOS XR software attempts to activate the primary pseudowire. The range, in seconds, is from 0 to 180. The default is 0.
never	Specifies that the secondary pseudowire does not fall back to the primary pseudowire if the primary pseudowire becomes available again, unless the secondary pseudowire fails.

Command Default

The default disable delay is the value of 0, which means that the primary pseudowire is activated immediately when it comes back up.

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how a backup delay is configured for point-to-point pseudowire in which the backup disable delay is set to 50 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class class1
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# backup disable delay 50
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# exit
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group A
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrx
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# neighbor 10.1.1.1 pw-id 2
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# pw-class class1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 95	Configures a pseudowire for a cross-connect.
p2p, on page 106	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 99	Enters pseudowire class submode to define a pseudowire class template.
xconnect group, on page 136	Configures cross-connect groups.

clear l2vpn collaborators

To clear the state change counters for L2VPN collaborators, use the **clear l2vpn collaborators** command in EXEC mode.

clear l2vpn collaborators

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to clear change counters for L2VPN collaborators:

```
RP/0/RSP0/CPU0:router# clear l2vpn collaborators
```

Related Commands

Command	Description
show l2vpn collaborators, on page 110	Displays information about the state of the interprocess communications connections between l2vpn_mgr and other processes.

clear l2vpn counters bridge mac-withdrawal

To clear the MAC withdrawal statistics for the counters of the bridge domain, use the **clear l2vpn counters bridge mac-withdrawal** command in EXEC mode.

clear l2vpn counters bridge mac-withdrawal {**all**| **group** *group-name* **bd-name** *bd-name*| **neighbor** *ip-address* **pw-id** *value*}

Syntax Description

all	Clears the MAC withdrawal statistics over all the bridges.
group *group-name*	Clears the MAC withdrawal statistics over the specified group.
bd-name *bd-name*	Clears the MAC withdrawal statistics over the specified bridge.
neighbor *ip-address*	Clears the MAC withdrawal statistics over the specified neighbor.
pw-id *value*	Clears the MAC withdrawal statistics over the specified pseudowire. The range is from 1 to 4294967295.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to clear the MAC withdrawal statistics over all the bridges:

```
RP/0/RSP0/CPU0:router# clear l2vpn counters bridge mac-withdrawal all
```

clear l2vpn forwarding counters

To clear L2VPN forwarding counters, use the **clear l2vpn forwarding counters** command in EXEC mode.

clear l2vpn forwarding counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to clear L2VPN forwarding counters:

```
RP/0/RSP0/CPU0:router# clear l2vpn forwarding counters
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

clear l2vpn forwarding message counters

To clear L2VPN forwarding message counters, use the **clear l2vpn forwarding message counters** command in EXEC mode.

clear l2vpn forwarding message counters location *node-id*

Syntax Description

location *node-id*	Clears L2VPN forwarding message counters for the specified location.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to clear L2VPN forwarding message counters on a specified node:

```
RP/0/RSP0/CPU0:router# clear l2vpn forwarding message counters location 0/6/CPU0
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

clear l2vpn forwarding table

To clear an L2VPN forwarding table at a specified location, use the **clear l2vpn forwarding table** command in EXEC mode.

clear l2vpn forwarding table location *node-id*

Syntax Description

location *node-id*	Clears L2VPN forwarding tables for the specified location.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to clear an L2VPN forwarding table from a specified location:

```
RP/0/RSP0/CPU0:router# clear l2vpn forwarding table location 1/2/3/5
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

control-word

To enable control word for MPLS encapsulation, use the **control-word** command in L2VPN pseudowire class encapsulation submode. To disable the control word, use the **no** form of this command.

control-word

no control-word

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN pseudowire class encapsulation configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to enable control word for MPLS encapsulation:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class pwc1
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)# control-word
```

dynamic-arp-inspection

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

dynamic-arp-inspection {**logging**| **address-validation** {*src-mac*| *dst-mac*| *ipv4*}}

no dynamic-arp-inspection {**logging**| **address-validation** {*src-mac*| *dst-mac*| *ipv4*}}

Syntax Description

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

Command Default

Dynamic ARP inspection is disabled.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection logging
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection address-validation
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

flood mode

To change the flood mode from Bandwidth Optimized to Convergence Optimized, use the **flood mode convergence-optimized** command in the l2vpn bridge group bridge domain configuration mode. To return the bridge to normal flooding behavior (when all unknown unicast, broadcast and multicast packets are flooded over other bridge domain network interfaces), use the **no** form of this command.

flood mode {**resilience-optimized| convergence-optimized**}

no flood mode {**resilience-optimized| convergence-optimized**}

Syntax Description

resilience-optimized	Configures bridge to use Resilience Optimized mode.
convergence-optimized	Configures bridge to use Convergence Optimized mode.

Command Default

The bridge domain operates in the Bandwidth Optimized Mode.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **flood mode** command allows you to change the flood optimization mode to either Convergence Optimized mode or Resilience Optimized mode. The Convergence Optimized mode floods all traffic to all line cards; all unknown unicast packets, all broadcast packets, and all multicast packets are flooded over all other bridge domain network interfaces. The Resilience Optimized Mode works like Bandwidth Optimized mode, except that it floods traffic to both primary and backup FRR links for a Pseudowire.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to clear an L2VPN forwarding table from a specified location:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group MyGroup
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain MyDomain
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# flood mode convergence-optimized
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.

interface (p2p)

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

interface *type interface-path-id*

no interface *type interface-path-id*

Syntax Description

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

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group gr1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p p001
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interface TenGigE 1/1/1/1
```

Related Commands

Command	Description
p2p, on page 106	Enters p2p configuration submode to configure point-to-point cross-connects.

ip-source-guard

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

ip-source-guard logging

no ip-source-guard logging

Syntax Description

logging	(Optional) Enables logging.

Command Default

IP Source Guard is disabled.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# ip-source-guard
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ipsg)#
```

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group b1
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# ip-source-guard logging
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ipsg)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

l2transport

To configure a physical interface to operate in Layer 2 transport mode, use the **l2transport** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

l2transport

no l2transport

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The l2transport command and these configuration items are mutually exclusive:

- IPv4 address and feature (for example, ACL) configuration
- IPv4 enable, address and feature (for example, ACL) configuration
- Bundle-enabling configuration
- L3 subinterfaces
- Layer 3 QoS Policy

Note After an interface or connection is set to Layer 2 switched, commands such as **ipv4 address** are not usable. If you configure routing commands on the interface, **l2transport** is rejected.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

Ethernet Port Mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-if)# l2transport
```

Ethernet VLAN Mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0.900 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 100do1q vlan 999
```

Ethernet VLAN Mode (QinQ):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0.900 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 20 second-dot1q 10vlan 999 888
```

Ethernet VLAN Mode (QinAny):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0.900 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 30 second-dot1q do1q vlan 999 any
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

l2transport l2protocol

To configure Layer 2 protocol handling, use the **l2transport l2protocol** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

l2transport l2protocol cpsv {**reverse-tunnel**| **tunnel**}

no l2transport l2protocol cpsv {**reverse-tunnel**| **tunnel**}

Syntax Description

cpsv	Enables L2PT for the interface. L2PT is enabled for the following protocols only: • CDP • STP • VTP **Note** STP includes all Spanning Tree protocol derivatives (RSTP, MSTP, etc.)
tunnel	Performs L2PT encapsulation on frames as they enter the interface. Also, performs L2PT de-encapsulation on frames as they exit they interface. L2PT encapsulation rewrites the destination MAC address with the L2PT destination MAC address. L2PT deencapsulation replaces the L2PT destination MAC address with the original destination MAC address.
reverse-tunnel	Performs L2PT encapsulation on frames as they exit the interface. Also, perform L2PT deencapsulation on frames as they enter the interface.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

These L2 protocols are available:

- Cisco Discovery Protocol (CDP)—CDP is protocol-independent and is used to obtain protocol addresses, platform information, and other data about neighboring devices.
- PVST maintains a spanning tree instance for each VLAN configured in the network and permits a VLAN trunk to be forwarding for some VLANs and not for others. It can also load balance Layer 2 traffic by forwarding some VLANs on one trunk and other VLANs n others.
- Spanning-Tree Protocol (STP)—STP is a link management protocol that provides path redundancy in the network. For Ethernet networks to function properly, only one active path can exist between two stations.
- VLAN Trunk Protocol (VTP)—VTP is a Cisco-proprietary protocol that reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain.

Task ID

Task ID	Operations
l2vpn	read, write
atm	read, write

Examples

The following example shows how to configure Layer 2 protocol handling:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-if)# l2transport l2protocol cpsv reverse-tunnelstp drop
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

l2transport propagate

To propagate Layer 2 transport events, use the **l2transport propagate** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

l2transport propagate remote-status

no l2transport propagate remote-status

Syntax Description

remote-status	Propagates remote link status changes.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **l2transport propagate** command provides a mechanism for the detection and propagation of remote link failure for port mode EoMPLS.

To display the state of l2transport events, use the **show controller internal** command in *Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*

For more information about the Ethernet remote port shutdown feature, see *Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide*.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to propagate remote link status changes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-if)# l2transport propagate remote remote-status
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

l2transport service-policy

To configure a Layer 2 transport quality of service (QoS) policy, use the **l2transport service-policy** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

l2transport service-policy {**input** *policy-name*| **output** *policy-name*}

no l2transport service-policy {**input** *policy-name*| **output** *policy-name*}

Syntax Description

input *policy-name*	Configures the direction of service policy application: input.
output *policy-name*	Configures the direction of service policy application: output.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write
atm	read, write

Examples

The following example shows how configure an L2 transport quality of service (QoS) policy:

```
RP/0/RSP0RP00/CPU0:router# configure
RP/0/RSP0RP00/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/RSP0RP00/CPU0:router(config-if)# l2transport service-policy input sp_0001
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

l2vpn

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

l2vpn

no l2vpn

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enter L2VPN configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

load-balancing flow

To enable all bundle EFPs and PW to use either L2 flow based or L3 flow based balancing, use the **load-balancing flow** command in L2VPN configuration mode.

load-balancing flow [**src-dst-mac**| **src-dst-ip**]

Syntax Description

src-dst-mac	Enables global flow load balancing hashed on source and destination MAC addresses.
src-dst-ip	Enables global flow load balancing hashed on source and destination IP addresses.

Command Default

None

Command Modes

L2VPN configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to set the bridge ID:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# load-balancing flow src-dst-ip
```

load-balancing flow-label

To balance the load based on flow-labels, use the **load balancing flow label** command in l2vpn pseudowire class mpls configuration mode. To undo flow-label based load-balancing, use the **no** form of this command.

load-balancing flow-label {**both**| **receive**| **transmit**}[**static**]

no load-balancing flow-label {**both**| **receive**| **transmit**}[**static**]

Syntax Description

both	Inserts or discards flow labels on transmit or receive.
receive	Discards flow label on receive.
transmit	Inserts flow label on transmit.
static	Sets flow label parameters statically.

Command Default

None

Command Modes

L2vpn pseudowire class mpls configuration mode

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows the output of the **load-balancing flow-label** command of the **both** keyword.

```
RP/0/RSP0/CPU0:router#config
RP/0/RSP0/CPU0:router(config)#l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#pw-class p1
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)#encapsulation
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)#encapsulation mpls
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)#load-balancing
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)#load-balancing flow-label
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)#load-balancing flow-label both
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)#load-balancing flow-label both static
```

Related Commands

Command	Description
pw-class encapsulation mpls, on page 103	Configures MPLS pseudowire encapsulation.

load-balancing pw-label

To enable all pseudowires using the defined class to use virtual circuit based load balancing, use the **load-balancing pw-label** command in pseudowire class configuration mode.

load-balancing pw-label

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Pseudowire class configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to set the bridge ID:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class abc
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)# load-balancing pw-label
```

logging (l2vpn)

To enable cross-connect logging, use the **logging** command in L2VPN configuration submode. To return to the default behavior, use the **no** form of this command.

logging pseudowire status

no logging pseudowire status

Syntax Description

pseudowire status	Enables pseudowire state change logging.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable cross-connect logging:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# logging pseudowire status
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.

monitor-session (l2vpn)

To attach a traffic monitoring session as one of the segments for a cross connect, use the **monitor-session** command in point-to-point cross connect configuration mode. To remove the association between a traffic mirroring session and a cross connect, use the **no** form of this command.

monitor-session *session-name*

no monitor-session *session-name*

Syntax Description

session-name	Name of the monitor session to configure.

Command Default

No default behavior or values

Command Modes

Point-to-point cross connect configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Before you can attach a traffic mirroring session to a cross connect, you must define it using the **monitor-session** global configuration command. Once the traffic mirroring session is defined, use the **monitor-session** point-to-point cross connect configuration command to attach this session as one of the segments for the cross connect. Once attached, all traffic replicated from the monitored interfaces (in other words, interfaces that are associated with the monitor-session) is replicated to the pseudowire that is attached to the other segment of the cross-connect.

The *session-name* argument should be different than any interface names currently used in the system.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to attach a traffic mirroring session as segment for the xconnect:

```
RP/0/RSP0/CPU0:router(config)# l2vpn
```

```
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group g1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p xcon1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# monitor-session mon1
```

Related Commands

Command	Description
monitor-session	Defines a traffic mirroring session and enter monitor session configuration mode.

mpls static label (L2VPN)

To configure static labels for MPLS L2VPN, use the **mpls static label** command in L2VPN cross-connect P2P pseudowire configuration mode. To have MPLS assign a label dynamically, use the **no** form of this command.

mpls static label local *label* **remote** *value*

no mpls static label local *label* **remote** *value*

Syntax Description

local *label*	Configures a local pseudowire label. Range is 16 to 15999.
remote *value*	Configures a remote pseudowire label. Range is 16 to 15999.

Command Default

The default behavior is a dynamic label assignment.

Command Modes

L2VPN cross-connect P2P pseudowire configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure static labels for MPLS L2VPN:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# mpls static label local 800 remote 500
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 95	Configures a pseudowire for a cross-connect.
p2p, on page 106	Enters p2p configuration submode to configure point-to-point cross-connects.
xconnect group, on page 136	Configures cross-connect groups.

neighbor (L2VPN)

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

neighbor *A.B.C.D* **pw-id** *value* [**backup**| **mpls** || **pw-class**]

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

Syntax Description

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

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

A cross-connect may have two segments:

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000 pw-class class12
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor 10.1.1.3 pw-id 1001 pw-class class13
RP/0/RSP0/CPU0:router(config-xc)# p2p rtrC_to_rtrD
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor 10.2.2.3 pw-id 200 pw-class class23
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor 10.2.2.4 pw-id 201 pw-class class24
```

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000 pw-class foo
RP/0/RSP0/CPU0:router(config-xc)# p2p rtrC_to_rtrD
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor 20.2.2.3 pw-id 200 pw-class bar1
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
p2p, on page 106	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 99	Enters pseudowire class submode to define a pseudowire class template.
xconnect group, on page 136	Configures cross-connect groups.

preferred-path

To configure an MPLS TE tunnel to be used for L2VPN traffic, use the **preferred-path** command in Encapsulation MPLS configuration mode. To delete the preferred-path, use the **no** form of this command.

preferred-path interface {**tunnel-ip** | **tunnel-te** | **tunnel-tp** }*value* [**fallback disable**]

no preferred-path interface {**tunnel-ip** | **tunnel-te** | **tunnel-tp** }*value* [**fallback disable**]

Syntax Description

interface	Interface for the preferred path.
tunnel-ip	IP tunnel interface name for the preferred path.
value	Tunnel number for preferred path.
fallback disable	(Optional) Disables fallback for preferred path tunnel settings.
tunnel te	Specifies the TE tunnel interface name for the preferred path.
tunnel tp	Specifies the TP tunnel interface name for the preferred path.

Command Default

None

Command Modes

Encapsulation MPLS configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	The keyword **tunnel-tp** was introduced.

Usage Guidelines

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

The **preferred-path** command is applicable only to pseudowires with MPLS encapsulation.

Use the **show l2vpn xconnect detail** command to show the status of fallback (that is, enabled or disabled).

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 configure preferred-path tunnel settings:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-tp 345

RP/0/RSP0/CPU0:router(config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-tp 345
 fallback disable
```

Related Commands

Command	Description
show l2vpn xconnect, on page 126	Displays brief information on configured cross-connects.

pw-class (L2VPN)

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

pw-class *class-name*

no pw-class *class-name*

Syntax Description

class-name	Pseudowire class name.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group l1vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# pw-class kanata01
```

Related Commands

Command	Description
p2p, on page 106	Enters p2p configuration submode to configure point-to-point cross-connects.

pw-class encapsulation l2tpv3

To configure L2TPv3 pseudowire encapsulation, use the **pw-class encapsulation l2tpv3** command in L2VPN pseudowire class configuration mode. To return to the default behavior, use the **no** form of this command.

pw-class class name encapsulation l2tpv3 [**cookie size** {**0**| **4**| **8**}| **ipv4 source** *address*| **pmtu max** *68-65535*| **protocol l2tpv3 class** *name*| **tos** {**reflect value** *0-255*| **value** *0-255*}| **ttl** *value*]

no pw-class class name encapsulation l2tpv3 [**cookie size** {**0**| **4**| **8**}| **ipv4 source** *address*| **pmtu max** *68-65535*| **protocol l2tpv3 class** *name*| **tos** {**reflect value** *0-255*| **value** *0-255*}| **ttl** *value*]

Syntax Description

class name	Configures an encapsulation class name.
cookie size {0 | 4 | 8}	(Optional) Configures the L2TPv3 cookie size setting: • 0—Cookie size is 0 bytes. • 4—Cookie size is 4 bytes. • 8—Cookie size is 8 bytes.
ipv4 source *address*	(Optional) Configures the local source IPv4 address.
pmtu max *68-65535*	(Optional) Configures the value of the maximum allowable session MTU.
protocol l2tpv3 class *name*	(Optional) Configures L2TPv3 as the signaling protocol for the pseudowire class.
tos {**reflect value** *0-255* | **value** *0-255*}	(Optional) Configures TOS and the TOS value. Range is 0 to 255.
ttl *value*	Configures the Time-to-live (TTL) value. Range is 1 to 255.

Command Default

None

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to define L2TPV3 pseudowire encapsulation:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation l2tpv3
```

The following example shows how to set the encapsulation and protocol to L2TPV3:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation l2tpv3
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-l2tpv3)# protocol l2tpv3
```

Related Commands

Command	Description
pw-class (L2VPN), on page 99	Enters pseudowire class submode to define a pseudowire class template.
pw-class encapsulation mpls, on page 103	Configures MPLS pseudowire encapsulation.

pw-class encapsulation mpls

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

pw-class *class-name* **encapsulation mpls** {**control word| ipv4| load-balancing flow-label| preferred-path| protocol ldp| redundancy one-way| sequencing| switching tlv| tag-rewrite| transport-mode| vccv verification-type none**}

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	The following keywords were added: • **preferred-path** • **sequencing** • **switching tlv** • **tag-rewrite** • **transport-mode**
Release 4.2.0	The keyword **redundancy one-way** was introduced.
Release 4.3.0	The keyword **load-balancing flow-label** was introduced.

Usage Guidelines

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

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:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation mpls
```

Related Commands

Command	Description
pw-class (L2VPN), on page 99	Enters pseudowire class submode to define a pseudowire class template.

p2p

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

p2p *xconnect-name*

no p2p *xconnect-name*

Syntax Description

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

Command Default

None

Command Modes

L2VPN xconnect

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group group 1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p xc1
```

Related Commands

Command	Description
interface (p2p), on page 71	Configures an attachment circuit.

sequencing (L2VPN)

To configure L2VPN pseudowire class sequencing, use the **pw-class sequencing** command in L2VPN pseudowire class encapsulation mode. To return to the default behavior, use the **no** form of this command.

sequencing {**both**| **receive**| **transmit {resynch 5-65535}**}

no sequencing {**both**| **receive**| **transmit {resynch 5-65535}**}

Syntax Description

both	Configures transmit and receive side sequencing.
receive	Configures receive side sequencing.
transmit	Configures transmit side sequencing.
resynch *5-65535*	Configures the threshold for out-of-sequence packets before resynchronization. Range is 5 to 65535.

Command Default

None

Command Modes

L2VPN pseudowire class encapsulation mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Do not configure **sequence resynch** on high speed circuits. On low speed circuits, do not configure a threshold lower than 10 to 20 seconds of traffic.

Note This command is not supported on the Cisco ASR 9000 Series Aggregation Services Router.

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure L2VPN pseudowire class sequencing:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/RSP0/CPU0:router(config-l2vpn-pw)# encapsulation mpls
RP/0/RSP0/CPU0:router(config-l2vpn-encap-mpls)# sequencing both
```

Related Commands

Command	Description
pw-class (L2VPN), on page 99	Enters pseudowire class submode to define a pseudowire class template.

show l2vpn collaborators

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

show l2vpn collaborators

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn collaborators
L2VPN Collaborator stats:
Name                  State       Up Cnts      Down Cnts
--------------------  ----------  -----------  -----------
IMC                    Down          0            0
LSD                    Up            1            0
```

This table describes the significant fields shown in the display.

Table 1: show l2vpn collaborators Field Descriptions

Field	Description
Name	Abbreviated name of the task interacting with l2vpn_mgr.

Field	Description
State	Indicates if l2vpn_mgr has a working connection with the other process.
Up Cnts	Number of times the connection between l2vpn_mgr and the other process has been successfully established.
Down Cnts	Number of times that the connection between l2vpn_mgr and the other process has failed or been terminated.

Related Commands

Command	Description
clear l2vpn collaborators, on page 61	Clears the state change counters for L2VPN collaborators.

show l2vpn discovery

To display discovery label block information, use the **show l2vpn discovery** command in EXEC mode.

show l2vpn discovery {**bridge-domain**| **xconnect**| **summary**| **private**}

Syntax Description

bridge-domain	Displays bridge domain related forwarding information.
xconnect	Displays VPWS edge information.
summary	Displays summary information.
private	Displays private log or trace information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples display output for the **show l2vpn discovery** command with bridge-domain filter:

```
RP/0/RSP0/CPU0:router#show l2vpn discovery bridge-domain

Service Type: VPLS,  Connected
  List of VPNs (8001 VPNs):

  Bridge group: bg1, bridge-domain: bg1_bd1, id: 0, signaling protocol: LDP
    VPLS-ID: (auto) 1:101
    Local L2 router id: 10.10.10.10
    List of Remote NLRI (3 NLRIs):
    Local Addr       Remote Addr      Remote L2 RID    Time Created
    ---------------- ---------------- ---------------- --------------------
    10.10.10.10      20.20.20.20      20.20.20.20      03/13/2010 21:27:05
    10.10.10.10      30.30.30.30      30.30.30.30      03/13/2010 21:27:05
    10.10.10.10      40.40.40.40      40.40.40.40      03/13/2010 21:27:05
```

The following examples display output for the **show l2vpn discovery summary** command:

```
RP/0/RSP0/CPU0:router#show l2vpn discovery summary
Sun Mar 14 15:13:31.240 EDT
BGP: connected=yes,  active=yes,  stdby=yes
Services
  Bridge domain: registered=yes, Num VPNs=8001
   Num Local Edges=8001, Num Remote Edges=24001, Num Received NLRIs=24001
  Xconnect: registered=yes, Num VPNs=0
   Num Local Edges=0, Num Remote Edges=0, Num Received NLRIs=0
```

Related Commands

Command	Description
show l2vpn bridge-domain (VPLS), on page 224	Display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains.

show l2vpn forwarding

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

show l2vpn forwarding {**bridge-domain**| **counter**| **detail**| **hardware**| **inconsistent**| **interface**| **l2tp**| **location** [*node-id*]| **message**| **mstp**| **pwgroup**| **resource**| **retry-list**| **summary**| **unresolved**}

Syntax Description

bridge-domain	Displays bridge domain related forwarding information.
counter	Displays the cross-connect counters.
detail	Displays detailed information from the layer2_fib manager.
hardware	Displays hardware-related layer2_fib manager information.
inconsistent	Displays inconsistent entries only.
interface	Displays the match AC subinterface.
l2tp	Displays L2TPv3 related forwarding information.
location *node-id*	Displays layer2_fib manager information for the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.
message	Displays messages exchanged with collaborators.
mstp	Displays multi-spanning tree related forwarding information.
pwgroup	Displays PW-Group related forwarding information.
resource	Displays resource availability information in the layer2_fib manager.
retry-list	Displays retry list related information.

summary	Displays summary information about cross-connects in the layer2_fib manager.
unresolved	Displays unresolved entries only.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding location 0/2/cpu0
Bridge-domain name: bg1:bd1, id: 0, state: up
 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
 Security: disabled
 DHCPv4 snooping: profile not known on this node
 IGMP snooping: disabled, flooding: disabled
 Bridge MTU: 1500 bytes
 Number of bridge ports: 1
 Number of MAC addresses: 0
 Multi-spanning tree instance: 0

  GigabitEthernet0/1/0/1.2, state: oper up
    Number of MAC: 0
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
    Storm control drop counters:
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0


Bridge-domain name: bg1:bd2, id: 1, state: up
  Type:  pbb-edge, I-SID: 1234
  Core-bridge: pbb-bd2
 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
 Security: disabled
 DHCPv4 snooping: profile not known on this node
 IGMP snooping: disabled, flooding: disabled
 Bridge MTU: 1500 bytes
 Number of bridge ports: 0
 Number of MAC addresses: 0
 Multi-spanning tree instance: 0

 PBB Edge, state: up
    Number of MAC: 0
 GigabitEthernet0/1/0/1.3, state: oper up
    Number of MAC: 0
    Storm control drop counters:
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0

Bridge-domain name: bg1:bd3, id: 2, state: up
  Type:  pbb-core
  Number of associated pbb-edge BDs: 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
 Security: disabled
 DHCPv4 snooping: profile not known on this node
 IGMP snooping: disabled, flooding: disabled
 Bridge MTU: 1500 bytes
 Number of bridge ports: 0
 Number of MAC addresses: 0
 Multi-spanning tree instance: 0

  PBB Core, state: up
  Vlan-id: 1

  GigabitEthernet0/1/0/1.4, state: oper up
    Number of MAC: 0
    Storm control drop counters:
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0
```

The following sample outputs shows the backup pseudowire information:

```
RP/0/RSP0/CPU0:router#show l2vpn forwarding detail location 0/2/CPU0
Local interface: GigabitEthernet0/2/0/0.1, Xconnect id: 0x3000001, Status: up
  Segment 1
    AC, GigabitEthernet0/2/0/0.1, Ethernet VLAN mode, status: Bound
    RG-ID 1, active
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
  Segment 2
    MPLS, Destination address: 101.101.101.101, pw-id: 1000, status: Bound
    Pseudowire label: 16000
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
  Backup PW
    MPLS, Destination address: 102.102.102.102, pw-id: 1000, status: Bound
    Pseudowire label: 16001
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0

RP/0/RSP0/CPU0:router#show l2vpn forwarding bridge-domain detail location 0/2/CPU0
Bridge-domain name: bg1:bd1, id: 0, state: up
….
  GigabitEthernet0/2/0/0.4, state: oper up
    RG-ID 1, active
    Number of MAC: 0
    …..

  Nbor 101.101.101.101 pw-id 5000
    Backup Nbor 101.101.101.101 pw-id 5000
    Number of MAC: 0
….
```

The following sample outputs displays the SPAN segment information of the xconnect:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding counter location 0/7/CPU0
Legend: ST = State, DN = Down

Segment 1                             Segment 2           ST     Byte
                                                                               Switched
----------------------------- -----------------------    --      ---------
pw-span-test (Monitor-Session) mpls  2.2.2.2  UP       0

RP/0/RSP0/CPU0:router #Show l2vpn forwarding monitor-session location 0/7/CPU0
Segment 1                            Segment 2                            State
------------------------------------ ------------------------------------ ------
pw-span-test(monitor-session)  mpls    2.2.2.2                      UP
pw-span-sess(monitor-session) mpls    3.3.3.3                      UP

RP/0/RSP0/CPU0:router #Show l2vpn forwarding monitor-session pw-span-test location 0/7/CPU0
Segment 1                                 Segment 2                            State
------------------------------------ ------------------------------------ ------
pw-span-test(Monitor-Session) mpls    2.2.2.2                      UP


Example 4:
RP/0/RSP0/CPU0:router #show l2vpn forwarding detail location 0/7/CPU0
  Xconnect id: 0xc000001, Status: up
  Segment 1
    Monitor-Session, pw-span-test, status: Bound
  Segment 2
    MPLS, Destination address: 2.2.2.2, pw-id: 1, status: Bound
    Pseudowire label: 16001
    Statistics:
      packets: received 0, sent 11799730
      bytes: received 0, sent 707983800

Example 5:
show l2vpn forwarding private location 0/11/CPU0
  Xconnect ID 0xc000001
  Xconnect info:
   Base info: version=0xaabbcc13, flags=0x0, type=2, reserved=0
    xcon_bound=TRUE, switching_type=0, data_type=3

  AC info:
   Base info: version=0xaabbcc11, flags=0x0, type=3, reserved=0
    xcon_id=0xc000001, ifh= none, subifh= none, ac_id=0, ac_type=SPAN,
    ac_mtu=1500, iw_mode=none, adj_valid=FALSE, adj_addr none


  PW info:
   Base info: version=0xaabbcc12, flags=0x0, type=4, reserved=0
    pw_id=1, nh_valid=TRUE, sig_cap_flags=0x20, context=0x0,
     MPLS, pw_label=16001
    Statistics:
      packets: received 0, sent 11799730
      bytes: received 0, sent 707983800

   Object: NHOP
   Event Trace History [Total events: 5]
--------------------------------------------------------------------
     Time                Event                Flags
     ====                =====                =====


--------------------------------------------------------------------


  Nexthop info:
   Base info: version=0xaabbcc14, flags=0x10000, type=5, reserved=0
    nh_addr=2.2.2.2, plat_data_valid=TRUE, plat_data_len=128, child_count=1

   Object: XCON
   Event Trace History [Total events: 16]
--------------------------------------------------------------------
     Time                Event                Flags
     ====                =====                =====

 -------------------------------------------------------------------
RP/0/RSP0/CPU0:router #show l2vpn forwarding summary location 0/7/CPU0
 Major version num:1, minor version num:0
Shared memory timestamp:0x31333944cf
Number of forwarding xconnect entries:2
  Up:2  Down:0
  AC-PW:1 (1 mpls)  AC-AC:0  AC-BP:0  AC-Unknown:0
  PW-BP:0  PW-Unknown:0 Monitor-Session-PW:1
Number of xconnects down due to:
  AIB:0  L2VPN:0  L3FIB:0
Number of p2p xconnects: 2
Number of bridge-port xconnects: 0
Number of nexthops:1
  MPLS:   Bound:1  Unbound:0  Pending Registration:0
Number of bridge-domains: 0
Number of static macs: 0
Number of locally learned macs: 0
Number of remotely learned macs: 0
Number of total macs: 0
```

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

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding location 0/2/cpu0

ID   Segment 1         Segment 2
-----------------------------------
1    Gi0/2/0/0 1       1.1.1.1   9)
```

The following sample output shows the MAC information in the layer2_fib manager summary:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding summary location 0/3/CPU0

Major version num:1, minor version num:0
Shared memory timestamp:0x66ff58e894
Number of forwarding xconnect entries:2
  Up:1  Down:0
  AC-PW:0  AC-AC:0  AC-BP:1 PW-BP:1
Number of xconnects down due to:
  AIB:0  L2VPN:0  L3FIB:0
Number of nexthops:1
Number of static macs: 5
Number of locally learned macs: 5
Number of remotely learned macs: 0
Number of total macs: 10
```

This example shows the sample output of a configured flow label:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding detail location 0/0/cPU0
Local interface: GigabitEthernet0/0/1/1, Xconnect id: 0x1000002, Status: up
  Segment 1
```

```
    AC, GigabitEthernet0/0/1/1, Ethernet port mode, status: Bound
    Statistics:
      packets: received 24849, sent 24847
      bytes: received 1497808, sent 1497637
  Segment 2
    MPLS, Destination address: 3.3.3.3, pw-id: 2, status: Bound, Active
    Pseudowire label: 16004    Control word disabled
    Backup PW
      MPLS, Destination address: 2.2.2.2, pw-id: 6, status: Bound
      Pseudowire label: 16000
    Flow label enabled
    Statistics:
      packets: received 24847, sent 24849
      bytes: received 1497637, sent 1497808
     Xconnect id: 0xff000014, Status: down
  Segment 1
    MPLS, Destination address: 2.2.2.2, pw-id: 1, status: Not bound
  Pseudowire label: UNKNOWN    Control word disabled
    Flow label enabled
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
  Segment 2
    Bridge id: 0, Split horizon group id: 0
    Storm control: disabled
    MAC learning: enabled
    MAC port down flush: 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
    Security: disabled
    DHCPv4 snooping: profile not known on this node, disabled
    IGMP snooping profile: profile not known on this node
    Router guard disabled
```

This example shows sample output for the **show l2vpn forwarding detail location** command with P2MP PW enabled on the PW BP.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding detail location
Xconnect id: 0xfffc0003, Status: up
  Segment 1
    MPLS, Destination address: 2.2.2.2, pw-id: 101, status: Bound
    Pseudowire label: 16002    Control word disabled
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
  Segment 2
    Bridge id: 0, Split horizon group id: 1
    Storm control: disabled
    MAC learning: enabled
    MAC port down flush: 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 Secure: disabled, Logging: disabled
    DHCPv4 snooping: profile not known on this node, disabled
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    IGMP snooping profile: profile not known on this node
    Router guard disabled
    P2MP PW enabled
```

This example shows sample output for the **show l2vpn forwarding summary location** command displaying number of bridge-domains with P2MP PW enabled.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding summary location
Mon Sep 9 22:07:54.000 EDT
Major version num:1, minor version num:0
Shared memory timestamp:0x547395c50
Global configuration:
Number of forwarding xconnect entries:5
  Up:0  Down:5
  AC-PW(atom):1 AC-PW(l2tpv2):0 AC-PW(l2tpv3):0
 (1 mpls)  AC-AC:0  AC-BP:0  AC-Unknown:0
  PW-BP:4  PW-Unknown:0
  PBB-BP:0  PBB-Unknown:0
  Monitor-Session-PW:0  Monitor-Session-Unknown:0
Number of xconnects down due to:
  AIB:0  L2VPN:5  L3FIB:0  VPDN:0
Number of xconnect updates dropped due to:
  Invalid XID: 0 VPWS PW, 0 VPLS PW, 0 Virtual-AC, 0 PBB
  Exceeded max allowed: 0 VPLS PW, 0 Bundle-AC
Number of p2p xconnects: 1
Number of bridge-port xconnects: 4
Number of nexthops:2
  MPLS:   Bound:2  Unbound:0  Pending Registration:0
  P2MP MLDP: Bound:1  Unbound:0  Pending Registration:0
  P2MP TE:   Bound:1  Unbound:0  Pending Registration:0
Number of bridge-domains: 2 (0 with routed interface, 2 with P2MP enabled)
Number of bridge-domain updates dropped: 0
Number of static macs: 0
Number of routed macs: 0
Number of locally learned macs: 0
Number of remotely learned macs: 0
Number of total macs: 0
Number of total P2MP Ptree entries: 2
  MLDP:1 (LMRIB:1) RSVP-TE:0 (LMRIB:0)
```

The example shows sample output for the **show l2vpn forwarding private** command with PW grouping for multi-segment PWs.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding private location
Tue Jun 18 22:25:36.142 DST
Xconnect ID 0x880001

  Xconnect info:
   Base info: version=0xaabbcc13, flags=0xc110, type=2, reserved=0
    xcon_bound=TRUE, switching_type=0, data_type=11

  AC info:
   Base info: version=0xaabbcc11, flags=0x0, type=3, reserved=0
    xcon_id=0x880001, ifh=0x2000580, subifh=0x2000042, ac_id=0, ac_type=21,
    ac_mtu=9000, iw_mode=1, adj_valid=TRUE, adj_addr 0x2000042
    r_aps_channel=FALSE, prot_exclusion=FALSE
    Statistics:
      packets: received 1, sent 2574
      bytes: received 68, sent 174990
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0

  PW info:
   Base info: version=0xaabbcc12, flags=0x0, type=4, reserved=0
    pw_id=100, nh_valid=TRUE, sig_cap_flags=0x20, context=0x0,
     MPLS, Destination address: 1.1.1.10, pw-id: 100, status: Bound, Active
    Pseudowire label: 16000    Control word disabled
    NHOP: 1.1.1.10, PW-Group Id: 0x1001
    Backup PW
      MPLS, Destination address: 3.3.3.30, pw-id: 300, status: Bound
      Pseudowire label: 0
      Redundancy role backup, not active, ready, flags 0x0
      NHOP: 3.3.3.30, Backup PW-Group Id: 0x1002

  Bridge port info:
   Base info: version=0xaabbcc1a, flags=0x0, type=12, reserved=0
    xcon_id=0x880001, bridge_id=1, shg_id=0, mac_limit=4000, mac_limit_action=0,
    bridge_ptr=0xa52bdc78, shg_ptr=0x0, msti_ptr=0xa52a10d8, segment_ptr=0xa52bd3a4
    segment_type=0x2, mtu=9000, msti=0, mvrp_seq_number=0
    is_flooding_disabled=FALSE, is_mac_learning_disabled=FALSE,
is_mac_port_down_flush_disabled=FALSE, mtu=9000, msti=0,
    aging_timeout=300, bridge_ptr=0xa52bdc78, shg_ptr=0x0, segment_type=2,
    segment_ptr=0xa52bd3a4
    MAC learning: enabled
    MAC port down flush: 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 Secure: disabled, Logging: disabled
    DHCPv4 snooping: profile not known on this node, disabled
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    IGMP snooping profile: profile not known on this node
    MLD snooping profile: profile not known on this node
    Router guard disabled
    STP participating: enabled
    Storm control: disabled
```

The example shows sample output for the **show l2vpn forwarding detail** command with PW grouping for multi-segment PWs.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding detail location
Local interface: GigabitEthernet0/0/0/0.100, Xconnect id: 0x100009, Status: up
  Segment 1
    AC, GigabitEthernet0/0/0/0.100, Ethernet VLAN mode, status: Bound
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
  Segment 2
    MPLS, Destination address: 1.1.1.10, pw-id: 100, status: Bound, Active
    Pseudowire label: 16000    Control word disabled
    NHOP: 1.1.1.10, PW-Group Id: 0x1001
    Backup PW
      MPLS, Destination address: 3.3.3.30, pw-id: 300, status: Bound
      Pseudowire label: 16000
      NHOP: 3.3.3.30, Backup PW-Group Id: 0x1002
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
```

The example shows sample output for the **show l2vpn forwarding summary** command with PW grouping for multi-segment PWs.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding summary location 0/0/CPU0
Tue Jun 18 22:29:47.815 DST
Major version num:1, minor version num:0
Shared memory timestamp:0x182a49b4f9
Global configuration:
Number of forwarding xconnect entries:31
  Up:19  Down:12
  AC-PW(atom):0 AC-PW(l2tpv2):0 AC-PW(l2tpv3):0
  AC-PW(l2tpv3-ipv6):0
  AC-AC:3  AC-BP:16  AC-Unknown:0
  PW-BP:12  PW-Unknown:0
  PBB-BP:0  PBB-Unknown:0
  Monitor-Session-PW:0  Monitor-Session-Unknown:0
Number of xconnects down due to:
  AIB:0  L2VPN:12  L3FIB:0  VPDN:0
Number of xconnect updates dropped due to:
  Invalid XID: 0 VPWS PW, 0 VPLS PW, 0 Virtual-AC, 0 PBB
  Exceeded max allowed: 0 VPLS PW, 0 Bundle-AC
Number of p2p xconnects: 1
Number of PW-Group Ids: 1
Number of PW-Group Ids Down: 0
Number of bridge-port xconnects: 28
Number of nexthops:5
  MPLS:   Bound:0  Unbound:5  Pending Registration:0
  P2MP MLDP: Bound:0  Unbound:0  Pending Registration:0
  P2MP TE:   Bound:0  Unbound:0  Pending Registration:0
Number of bridge-domains: 14
  2 with routed interface
  0 with PBB evpn enabled
  0 with p2mp enabled
Number of bridge-domain updates dropped: 0
Number of total macs: 0
  0 Static macs
  0 Routed macs
  0 BMAC
  0 Source BMAC
  0 Locally learned macs
  0 Remotely learned macs
Number of total P2MP Ptree entries: 0
Number of EVPN Multicast Replication lists: 0 (0 default)
```

The example shows sample output for the **show l2vpn forwarding pwgroup** command identifying the PWs of the same PW group as known by L2FIB.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding pwgroup ?
  debug      Include debug information(cisco-support)
  detail     Detailed information
  location   Specify a location
  peer-addr  PW-Group peer IPv4 address
  group-id   Provide information for the given PW-Group Id
```

The example shows sample output for the **show l2vpn forwarding pwgroup group-id** command with a specified group ID.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding pwgroup group-id 0x1001 loc 0/0/cpu0
Xconnect ID 0x1080001
 PW info:
   Base info: version=0xaabbcc12, flags=0x0, type=4, reserved=0
    pw_id=100, nh_valid=TRUE, sig_cap_flags=0x20, context=0x0,
     MPLS, Destination address: 1.1.1.10, pw-id: 100, status: Bound, Active
    Pseudowire label: 16000    Control word disabled
    Redundancy role: active, PW-Group Id 0x1001

Xconnect ID 0x1080008
 PW info:
   Base info: version=0xaabbcc12, flags=0x0, type=4, reserved=0
    pw_id=108, nh_valid=TRUE, sig_cap_flags=0x20, context=0x0,
     MPLS, Destination address: 1.1.1.10, pw-id: 108, status: Bound, Active
    Pseudowire label: 16000    Control word disabled
    Redundancy role none, PW-Group Id 0x1001
```

Related Commands

Command	Description
clear l2vpn forwarding counters, on page 63	Clears L2VPN forwarding counters.

show l2vpn pw-class

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

show l2vpn pw-class [**detail**| **name** *class name*]

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn pw-class

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

This table describes the significant fields shown in the display.

Table 2: show l2vpn pw-class Command Field Descriptions

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

Related Commands

Command	Description
clear l2vpn forwarding counters, on page 63	Clears L2VPN forwarding counters.

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

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn resource

Memory: Normal
```

describes the significant fields shown in the display.Table 3: show l2vpn resource Command Field Descriptions, on page 125

Table 3: show l2vpn resource Command Field Descriptions

Field	Description
Memory	Displays memory status.

show l2vpn xconnect

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

show l2vpn xconnect [**brief**| **detail**| *encapsulation*| **group**| **groups**| **interface**| **mp2mp**| **neighbor**| **pw-class**| **state**| **summary**| **type** {**ac-pw**| **locally-switched**| **monitor-session-pw**| **ms-pw**}]

Syntax Description

brief	(Optional) Displays encapsulation brief information.
detail	(Optional) Displays detailed information.
encapsulation	(Optional) Filters on encapsulation type.
group	(Optional) Displays all cross-connects in a specified group.
groups	(Optional) Displays all groups information.
interface	(Optional) Filters on interface and subinterface.
mp2mp	(Optional) Displays MP2MP information.
mpsw	(Optional) Displays ms_pw information.
neighbor	(Optional) Filters on neighbor.
private	(Optional) Displays private information.
pw-class	(Optional) Filters on pseudowire class
state	(Optional) Filters the following xconnect state types: • up • down
summary	(Optional) Displays AC information from the AC Manager database.
type	(Optional) Filters the following xconnect types: • ac-pw • locally switched • monitor-session-pw • ms-pw

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

If a specific cross-connect is specified in the command (for instance, AC_to_PW1) then only that cross-connect will be displayed; otherwise, all cross-connects are displayed.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect

Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
              LU = Local Up, RU = Remote Up, CO = Connected

XConnect                   Segment 1                   Segment 2
Group      Name       ST   Description            ST   Description            ST
----------------------------   ---------------------------   -------------------------
g1      x1        UP   pw-span-test          UP   2.2.2.2     1      UP

siva_xc    siva_p2p   UP   Gi0/4/0/1              UP   10.1.1.1         1      UP
                                                       Backup
                                                       10.2.2.2         2      UP
--------------------------------------------------------------------------------
```

The following sample output shows that the backup is in standby mode for the **show l2vpn xconnect detail** command:

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect detail

Group siva_xc, XC siva_p2p, state is up; Interworking none
 Monitor-Session: pw-span-test, state is configured
  AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none; MSTi 0
    Statistics:
      packet totals: send 90
      byte totals: send 19056
  PW: neighbor 10.1.1.1, PW ID 1, state is up ( established )
```

```
    PW class not set, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        30005                          16003
      Group ID     0x5000300                      0x5000400
      Interface    GigabitEthernet0/4/0/1         GigabitEthernet0/4/0/2
   Interface  pw-span-test          GigabitEthernet0/3/0/1
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ -----------------------------
    Create time: 20/11/2007 21:45:07 (00:49:18 ago)
    Last time status changed: 20/11/2007 21:45:11 (00:49:14 ago)
    Statistics:
      packet totals: receive 0
      byte totals: receive 0

  Backup PW:
  PW: neighbor 2.2.2.2, PW ID 2, state is up ( established )
    Backup for neighbor 1.1.1.1 PW ID 1 ( standby )
    PW class not set, XC ID 0x0
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        30006                          16003
      Group ID     unassigned                     0x5000400
      Interface    unknown                        GigabitEthernet0/4/0/2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ -----------------------------
    Backup PW for neighbor 10.1.1.1 PW ID 1
    Create time: 20/11/2007 21:45:45 (00:48:40 ago)
    Last time status changed: 20/11/2007 21:45:49 (00:48:36 ago)
    Statistics:
      packet totals: receive 0
      byte totals: receive 0
```

The following sample output shows that the backup is active for the **show l2vpn xconnect detail** command:

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect detail

Group siva_xc, XC siva_p2p, state is down; Interworking none
 Monitor-Session: pw-span-test, state is configured
  AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none; MSTi 0
    Statistics:
      packet totals: send 98
      byte totals: send 20798
  PW: neighbor 10.1.1.1, PW ID 1, state is down ( local ready )
    PW class not set, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        30005                          unknown
      Group ID     0x5000300                      0x0
      Interface    GigabitEthernet0/4/0/1         unknown
   Interface   pw-span-test          GigabitEthernet0/3/0/1
      MTU          1500                           unknown
      Control word enabled                        unknown
      PW type      Ethernet                       unknown
      VCCV CV type 0x2                            0x0
                                                  (none)
                   (LSP ping verification)
      VCCV CC type 0x3                            0x0
                                                  (none)
                    (control word)
                   (router alert label)
      ------------ ------------------------------ -----------------------------
    Create time: 20/11/2007 21:45:06 (00:53:31 ago)
    Last time status changed: 20/11/2007 22:38:14 (00:00:23 ago)
    Statistics:
      packet totals: receive 0
      byte totals: receive 0

  Backup PW:
  PW: neighbor 10.2.2.2, PW ID 2, state is up ( established )
    Backup for neighbor 10.1.1.1 PW ID 1 ( active )
    PW class not set, XC ID 0x0
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        30006                          16003
      Group ID     unassigned                     0x5000400
      Interface    unknown                        GigabitEthernet0/4/0/2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ -----------------------------
    Backup PW for neighbor 10.1.1.1 PW ID 1
    Create time: 20/11/2007 21:45:44 (00:52:54 ago)
    Last time status changed: 20/11/2007 21:45:48 (00:52:49 ago)
    Statistics:
      packet totals: receive 0
      byte totals: receive 0
```

The following sample output displays the xconnects with switch port analyzer (SPAN) as one of the segments:

```
Show l2vpn xconnect type minotor-session-pw
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        LU = Local Up, RU = Remote Up, CO = Connected

XConnect                         Segment 1                    Segment 2
Group           Name     ST     Description          ST   Description            ST
-----------------------------   ---------------------------  --------------------------
g1                x1        UP    pw-span-test          UP   2.2.2.2         1      UP
--------------------------------------------------------------------------------------
```

The following sample output shows that one-way redundancy is enabled:

```
Group g1, XC x2, state is up; Interworking none
  AC: GigabitEthernet0/2/0/0.2, state is up, active in RG-ID 1
    Type VLAN; Num Ranges: 1
    VLAN ranges: [2, 2]
    MTU 1500; XC ID 0x3000002; interworking none
    Statistics:
      packets: received 103, sent 103
      bytes: received 7348, sent 7348
      drops: illegal VLAN 0, illegal length 0
  PW: neighbor 101.101.101.101, PW ID 2000, state is up ( established )
    PW class class1, XC ID 0x3000002
    Encapsulation MPLS, protocol LDP
    PW type Ethernet VLAN, control word disabled, interworking none
PW backup disable delay 0 sec
One-way PW redundancy mode is enabled
    Sequencing not set
…..
    Incoming Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
    Outgoing Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
…..
  Backup PW:
  PW: neighbor 102.102.102.102, PW ID 3000, state is standby ( all ready )
    Backup for neighbor 101.101.101.101 PW ID 2000 ( inactive )
    PW class class1, XC ID 0x3000002
    Encapsulation MPLS, protocol LDP
    PW type Ethernet VLAN, control word disabled, interworking none
    Sequencing not set
…..
    Incoming Status (PW Status TLV):
      Status code: 0x26 (Standby, AC Down) in Notification message
    Outgoing Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
```

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

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect

Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
              LU = Local Up, RU = Remote Up, CO = Connected

XConnect                   Segment 1                   Segment 2
Group      Name       ST   Description            ST   Description            ST
----------------------------   --------------------------   -------------------------
siva_xc    siva_p2p   UP   Gi0/4/0/1              UP   1.1.1.1         1      UP
                                                       Backup
                                                       2.2.2.2         2      UP
--------------------------------------------------------------------------------
```

The following sample output shows that the backup is in standby mode for the **show l2vpn xconnect detail** command:

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect detail

Group siva_xc, XC siva_p2p, state is up; Interworking none
  AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none; MSTi 0
    Statistics:
      packet totals: received 90, sent 90
      byte totals: received 19056, sent 19056
  PW: neighbor 1.1.1.1, PW ID 1, state is up ( established )
    PW class not set, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        30005                          16003
      Group ID     0x5000300                      0x5000400
      Interface    GigabitEthernet0/4/0/1         GigabitEthernet0/4/0/2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
```

```
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ -----------------------------
    Create time: 20/11/2007 21:45:07 (00:49:18 ago)
    Last time status changed: 20/11/2007 21:45:11 (00:49:14 ago)
    Statistics:
      packet totals: received 0, sent 0
      byte totals: received 0, sent 0

  Backup PW:
  PW: neighbor 2.2.2.2, PW ID 2, state is up ( established )
    Backup for neighbor 1.1.1.1 PW ID 1 ( standby )
    PW class not set, XC ID 0x0
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        30006                          16003
      Group ID     unassigned                     0x5000400
      Interface    unknown                        GigabitEthernet0/4/0/2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ -----------------------------
    Backup PW for neighbor 1.1.1.1 PW ID 1
    Create time: 20/11/2007 21:45:45 (00:48:40 ago)
    Last time status changed: 20/11/2007 21:45:49 (00:48:36 ago)
    Statistics:
      packet totals: received 0, sent 0
      byte totals: received 0, sent 0
```

The following sample output shows that the backup is active for the **show l2vpn xconnect detail** command:

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect detail

Group siva_xc, XC siva_p2p, state is down; Interworking none
  AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none; MSTi 0
    Statistics:
      packet totals: send 98
      byte totals: send 20798
  PW: neighbor 1.1.1.1, PW ID 1, state is down ( local ready )
    PW class not set, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        30005                          unknown
      Group ID     0x5000300                      0x0
      Interface    GigabitEthernet0/4/0/1         unknown
      MTU          1500                           unknown
      Control word enabled                        unknown
      PW type      Ethernet                       unknown
      VCCV CV type 0x2                            0x0
                                                  (none)
                   (LSP ping verification)
      VCCV CC type 0x3                            0x0
                                                  (none)
                    (control word)
```

```
                  (router alert label)
      ------------ ------------------------------ -----------------------------
    Create time: 20/11/2007 21:45:06 (00:53:31 ago)
    Last time status changed: 20/11/2007 22:38:14 (00:00:23 ago)
    Statistics:
      packet totals: received 0, sent 0
      byte totals: received 0, sent 0

  Backup PW:
  PW: neighbor 2.2.2.2, PW ID 2, state is up ( established )
    Backup for neighbor 1.1.1.1 PW ID 1 ( active )
    PW class not set, XC ID 0x0
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        30006                          16003
      Group ID     unassigned                     0x5000400
      Interface    unknown                        GigabitEthernet0/4/0/2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ -----------------------------
    Backup PW for neighbor 1.1.1.1 PW ID 1
    Create time: 20/11/2007 21:45:44 (00:52:54 ago)
    Last time status changed: 20/11/2007 21:45:48 (00:52:49 ago)
    Statistics:
      packet totals: received 0, sent 0
      byte totals: received 0, sent 0
```

This example shows that the PW type changes to Ethernet, which is Virtual Circuit (VC) type 5, on the interface when a double tag rewrite option is used.

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect pw-class pw-class1 detail

Group VPWS, XC ac3, state is up; Interworking none
AC: GigabitEthernet0/7/0/5.3, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [12, 12]
MTU 1508; XC ID 0x2440096; interworking none
Statistics:
packets: received 26392092, sent 1336
bytes: received 1583525520, sent 297928
drops: illegal VLAN 0, illegal length 0
PW: neighbor 3.3.3.3, PW ID 3, state is up ( established )
PW class VPWS1, XC ID 0x2440096
Encapsulation MPLS, protocol LDP
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

Preferred path tunnel TE 3, fallback disabled
PW Status TLV in use
      MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        16147                          21355
      Group ID     0x120001c0                     0x120001c0
      Interface    GigabitEthernet0/7/0/5.3       GigabitEthernet0/7/0/5.3
      MTU          1508                           1508
      Control word disabled                       disabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x6                            0x6
                   (router alert label)           (router alert label)
                   (TTL expiry)                   (TTL expiry)
      ------------ ------------------------------ -----------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 4294705365
Create time: 21/09/2011 08:05:01 (00:14:01 ago)
Last time status changed: 21/09/2011 08:07:01 (00:12:01 ago)
Statistics:
packets: received 1336, sent 26392092
bytes: received 297928, sent 1583525520
```

This example shows the sample output of a configured flow label:

```
RP/0/RSP0/CPU0:router#  show l2vpn xconnect detail
Group g1, XC p1, state is up; Interworking none
  AC: GigabitEthernet0/0/1/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x1000002; interworking none
    Statistics:
      packets: received 24688, sent 24686
      bytes: received 1488097, sent 1487926
  PW: neighbor 3.3.3.3, PW ID 2, state is up ( established )
    PW class class1, XC ID 0x1000002
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word disabled, interworking none
    PW backup disable delay 0 sec
Sequencing not set
Flow label flags configured (Rx=1,Tx=1), negotiated (Rx=0,Tx=1)
```

This table describes the significant fields shown in the display.

Table 4: show l2vpn xconnect Command Field Descriptions

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

Related Commands

Command	Description
xconnect group, on page 136	Configures cross-connect groups.

transport mode (L2VPN)

To configure L2VPN pseudowire class transport mode, use the **transport mode** command in L2VPN pseudowire class MPLS encapsulation mode. To disable the L@VPN pseudowire class transport mode configuration, use the **no** form of this command.

transport mode {**ethernet**| **vlan** *passthrough* }

no transport mode {**ethernet**| **vlan** *passthrough* }

Syntax Description

ethernet	Configures Ethernet port mode.
vlan	Configures VLAN tagged mode.
passthrough	Enables the pseudowires to pass through the incoming tags.

Command Default

None

Command Modes

L2VPN pseudowire class MPLS encapsulation

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.1.0	The variable **passthrough** was introduced.

Usage Guidelines

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

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 configure Ethernet transport mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/RSP0/CPU0:router(config-l2vpn-pw)# encapsulation mpls
RP/0/RSP0/CPU0:router(config-l2vpn-encap-mpls)# transport-mode ethernet
```

Examples

The following example shows how to configure pseudowires in a VLAN tagged mode with the passthrough variable:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class pwc1
RP/0/RSP0/CPU0:router(config-l2vpn-pw)# encapsulation mpls
RP/0/RSP0/CPU0:router(config-l2vpn-encap-mpls)# transport-mode vlan passthrough
```

Related Commands

Command	Description
pw-class (L2VPN), on page 99	Enters pseudowire class submode to define a pseudowire class template.

xconnect group

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

xconnect group *group-name*

no xconnect group *group-name*

Syntax Description

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

Command Default

None

Command Modes

L2VPN configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group customer_atlantic
```

Related Commands

Command	Description
show l2vpn xconnect, on page 126	Displays brief information on configured cross-connects.

Multipoint Layer 2 Services Commands

action (VPLS)

To configure the bridge behavior when the number of learned MAC addresses reaches the MAC limit configured, use the **action** command in L2VPN bridge group bridge domain MAC limit configuration mode. To disable this feature, use the **no** form of this command.

action {**flood| no-flood| shutdown**}

no action {**flood| no-flood| shutdown**}

Syntax Description

flood	Configures the action to flood all unknown unicast packets when the MAC limit is reached. If the action is set to flood, all unknown unicast packets, with unknown destinations addresses, are flooded over the bridge.
no-flood	Configures the action to no-flood so all unknown unicast packets are dropped when the MAC limit is reached. If the action is set to no-flood, all unknown unicast packets, with unknown destination addresses, are dropped.
shutdown	Stops forwarding when the MAC limit is reached. If the action is set to shutdown, all packets are dropped.

Command Default

No action is taken when the MAC address limit is reached.

Command Modes

L2VPN bridge group bridge domain MAC limit configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **action** command to specify the type of action to be taken when the action is violated.

The configured action has no impact if the MAC limit has not been reached.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the bridge bar to flood all unknown unicast packets when the number of MAC addresses learned by the bridge reaches 10:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)#bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)#limit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)#action flood
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)#maximum 10
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
limit (VPLS), on page 182	Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 188	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 200	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

aging (VPLS)

To enter the MAC aging configuration submode to set the aging parameters such as time and type, use the **aging** command in L2VPN bridge group bridge domain configuration mode. To return to the default value for all parameters that are attached to this configuration submode, use the **no** form of this command.

aging

no aging

Syntax Description

This command has no keywords or arguments.

Command Default

No defaults are attached to this parameter since it is used as a configuration submode. See defaults that are assigned to the time (VPLS), on page 267 and the type (VPLS), on page 269 parameters.

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enter MAC aging configuration submode and to set the MAC aging time to 120 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# time 120
```

Related Commands

Commands	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then assigns network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
time (VPLS), on page 267	Configures the maximum aging time.
type (VPLS), on page 269	Configures the type for MAC address aging.

aps-channel

To configure G.8032 instance APS channel and to enter Ethernet ring G.8032 instance aps-channel configuration submode, use the **aps-channel** command in the Ethernet ring g8032 instance configuration submode. To remove the G.8032 instance APS channel configuration, use the **no** form of this command.

aps-channel [**level** *message-level*| **port0 interface** {**Bundle-Ether| FastEthernet| GigabitEthernet| TenGigE**} *interface-id* | **port1** {**bridge-domain** *bridge-domain-name*| **interface** {**Bundle-Ether| FastEthernet| GigabitEthernet| TenGigE**} *interface-id* **| none| xconnect** *xconnect-name*}]

no aps-channel [**level** *message-level*| **port0 interface** {**Bundle-Ether| FastEthernet| GigabitEthernet| TenGigE**} *interface-id* | **port1** {**bridge-domain** *bridge-domain-name*| **interface** {**Bundle-Ether| FastEthernet| GigabitEthernet| TenGigE**} *interface-id* **| none| xconnect** *xconnect-name*}]

Syntax Description

level	Specifies the APS message level. The message level ranges from 0 to 7.
port0	Configures G.8032 aps-channel information associated to port0.
port1	Configures G.8032 aps-channel information associated to port1.
interface	Assigns interface associated to port0 or port1. You can assign one of these interfaces: • Bundle Ethernet • Fast Ethernet • Gigabit Ethernet • TenGigabit Ethernet
bridge-domain	Specifies VPLS domain where virtual channel is connected.
none	Specify APS channel port0 or port1 as none.
xconnect	Specifies VPWS xconnect where virtual channel is connected.

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to configure G.8032 instance APS channel:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# instance 1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# description test
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# profile p1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# rpl port0 neighbor
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# inclusion-list vlan-ids e-g
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# aps-channel
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance-aps)#
```

Related Commands

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.
inclusion-list, on page 170	Associates a set of VLAN IDs with the current instance.

autodiscovery bgp

To enable BGP autodiscovery, use the **autodiscovery bgp** command in the VFI configuration mode. To return to the default value, use the **no** form of this command.

autodiscovery bgp

no autodiscovery bgp

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

VFI configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure a bridge domain:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EGroup
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain eastdomain
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi eastvfi
RP/0/RSP0/CPU0:routerr(config-l2vpn-bg-bd-vfi)# autodiscovery bgp
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

bridge-domain (VPLS)

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 mode. To return to a single bridge domain, use the **no** form of this command.

bridge-domain *bridge-domain-name*

no 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 3.7.2	This command was introduced.

Usage Guidelines

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

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:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#
```

Related Commands

Command	Description
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

bridge group (VPLS)

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 3.7.2	This command was introduced.

Usage Guidelines

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

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:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
l2vpn, on page 83	Enters L2VPN configuration mode.

clear l2vpn bridge-domain (VPLS)

To clear the MAC addresses and to restart the bridge domains on the router, use the **clear l2vpn bridge-domain** command in EXEC mode.

clear l2vpn bridge-domain {**all**| **bd-name** *name*| **group** *group*}

Syntax Description

all	Clears and restarts all the bridge domains on the router.
bd-name *name*	Clears and restarts the specified bridge domain. The *name* argument specifies the name of the bridge-domain.
group *group*	Clears and restarts all the bridge domains that are part of the bridge group.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

This is the method that allows a bridge to forward again after it was put in Shutdown state as a result of exceeding the configured MAC limit.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to clear all the MAC addresses and to restart all the bridge domains on the router:

```
RP/0/RSP0/CPU0:router# clear l2vpn bridge-domain all
```

Related Commands

Command	Description
show l2vpn bridge-domain (VPLS), on page 224	Display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains.

description (G.8032)

To specify a string that serves as a description for a G.8032 Ethernet ring instance, use the **description** command in the Ethernet ring G.8032 instance configuration submode.

description *ring-instance-identifier*

Syntax Description

ring-instance-identifier	A string that serves as a description for a G.8032 Ethernet ring instance. The string can be a maximum of 32 characters.

Command Default

None

Command Modes

Ethernet ring G.8032 instance configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to specify a description for G.8032 Ethernet ring instance:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# instance 1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# description test
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.
instance (G.8032), on page 172	Configures a G.8032 Ethernet ring instance and enters Ethernet ring G.8032 instance configuration submode.

dhcp ipv4 snoop profile (VPLS)

To enable DHCP snooping on a bridge and to attach a DHCP snooping profile to the bridge, use the **dhcp ipv4 snoop** command in L2VPN bridge group bridge domain configuration mode. To disable DHCP snooping on an interface, use the **no** form of this command.

dhcp ipv4 snoop profile *profile-name*

no dhcp ipv4 snoop

Syntax Description

profile *profile-name*	Attaches a DHCP profile. Profile name for DHCPv4 snooping.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable DHCP snooping on a bridge:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dhcp ipv4 snoop profile attach
```

This example shows how to enable DHCP snooping over a pseudowire:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#vfi vf1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)#exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#neighbor 10.1.1.1 pw-id 100
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)#dhcp ipv4 snoop profile A
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

ethernet ring g8032

To enable G.8032 ring mode and enter the G.8032 configuration submode, use the **ethernet ring g8032** command in the L2VPN configuration mode. To disable the G.8032 ring mode, use the **no** form of this command.

ethernet ring g8032 *protocol ring identifier*

no ethernet ring g8032 *protocol ring identifier*

Syntax Description

protocol ring identifier	Ring profile name. The maximum size of the profile name is 32 characters.

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to enable the G.8032 ring mode:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#ethernet ring g8032 p1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)#
```

Related Commands

Command	Description
exclusion list, on page 164	Defines a set of Virtual LAN (VLAN) IDs that are not protected by the Ethernet ring protection mechanism.
instance (G.8032), on page 172	Configures a G.8032 Ethernet ring instance and enters Ethernet ring G.8032 instance configuration submode.
port0 interface, on page 203	Enables G.8032 for a specified ring port.
port1, on page 205	Enables G.8032 for a specified ring port.

ethernet ring g8032 profile

To configure G.8032 ring profile and to enter the G.8032 ring profile configuration mode, use the **ethernet ring g8032 profile**command in the global configuration mode. To disable the G.8032 ring profile, use the **no** form of this command.

ethernet ring g8032 profile *profile-name* [**non-revertive**| **timer** {**guard** *milliseconds*| **hold-off** *seconds*| **wtr** *minutes* }]

Syntax Description

non-revertive	Configures non-revertive ring instance.
timer	Configures G.8032 timer.
guard	Configures G.8032 guard timer. The Guard timer can be configured and the default time interval is 500 ms. The time interval ranges from 10 to 2000 ms.
hold-off	Configures G.8032 hold-off timer. The hold-off timer can be configured and the default time interval is 0 seconds. The time interval ranges from 0 to 10 seconds.
wtr	Configures G.8032 WTR timer. The WTR timer can be configured by the operator, and the default time interval is 5 minutes. The time interval ranges from 1 to 12 minutes.

Command Default

None

Command Modes

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ethernet-services	read, write

Examples

This example shows you how to configure a G.8032 ring profile:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet ring g8032 profile p1
RP/0/RSP0/CPU0:router(config-g8032-ring-profile)#
```

Related Commands

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

exclusion list

To define a set of Virtual LAN (VLAN) IDs that are not protected by the Ethernet ring protection mechanism, use the **exclusion list** command in Ethernet ring g8032 configuration submode. To delete the set of VLAN IDs, use the **no** form of this command.

exclusion list vlan-ids *vlan range*

no exclusion list vlan-ids *vlan range*

Syntax Description

vlan-ids	Specifies a list of VLANs. Ranges in the form a-b,c,d,e-f,g where VLAN value is 1–4094 and/or untagged. By default, all the VLANs configured under ring ports are blocked. VLAN IDs specified here cannot belong to the inclusion-list. VLAN IDs range cannot overlap with the IDs specified under inclusion-list.

Command Default

Configured physical Ethernet or ether bundle interface

Command Modes

Ethernet ring g8032 configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows the output from the exclusion list command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# exclusion-list vlan-ids e-g
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-erp)#
```

Related Commands

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

flooding disable

To configure flooding for traffic at the bridge domain level or at the bridge port level, use the **flooding disable** command in L2VPN bridge group bridge domain configuration mode. To return the bridge to normal flooding behavior when all unknown unicast packets, all broadcast packets, and all multicast packets are flooded over all other bridge domain network interfaces, use the **no** form of this command.

flooding disable

no flooding disable

This command has no keywords or arguments.

Command Default

The default behavior is that packets are flooded when their destination MAC address is not found.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **flooding disable** command to override the parent bridge configuration.

By default, bridge ports inherit the flooding behavior of the bridge domain.

When flooding is disabled, all unknown unicast packets, all broadcast packets, and all multicast packets are discarded.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to disable flooding on the bridge domain called bar:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# flooding disable
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mtu (VPLS), on page 196	Adjusts the maximum packet size or maximum transmission unit (MTU) size for the bridge domain.

flooding unknown-unicast disable (VPLS)

To disable flooding of unknown unicast traffic at the bridge domain level or at the bridge port level, use the **flooding unknownunknow-unicast disable** command in L2VPN bridge group bridge domain configuration mode. To return the bridge to normal flooding behavior, use the **no** form of this command.

flooding unknown-unicast disable

no flooding unknown-unicast disable

Syntax Description

This command has no keywords or arguments.

Command Default

The default behavior is that packets are flooded when their destination MAC address is not found.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Use the **flooding unknown-unicast disable** command to override the parent bridge configuration.

By default, bridge ports inherit the flooding behavior of the bridge domain.

When flooding is disabled, all unknown unicast packets are discarded.

Use this command on Layer 2 interfaces. This command is not applicable on BVI interfaces.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to disable flooding on the bridge domain called bar:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# flooding unknown-unicast disable
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mtu (VPLS), on page 196	Adjusts the maximum packet size or maximum transmission unit (MTU) size for the bridge domain.

inclusion-list

To associate a set of VLAN IDs with the current instance, use the **inclusion-list** command in the Ethernet ring G.8032 instance configuration submode. To disassociate the VLAN IDs with the current instance, use the **no** form of this command.

inclusion-list vlan-ids*vlan-id*

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

Syntax Description

vlan-ids	Associates a set of VLAN IDs with the current instance.
vlan-id	List of VLAN IDs in the form vlan-id <vlan range>[,<vlan range][,<vlan range>][,<vlan range>].

Command Default

None

Command Modes

Ethernet ring G.8032 instance configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to associate VLAN IDs with instance 1:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# instance 1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# description test
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# profile p1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# rpl port0 neighbor
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# inclusion-list vlan-ids e-g
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.
instance (G.8032), on page 172	Configures a G.8032 Ethernet ring instance and enters Ethernet ring G.8032 instance configuration submode.

instance (G.8032)

To configure a G.8032 Ethernet ring instance and enter Ethernet ring G.8032 instance configuration submode, use the instance command in the Ethernet ring G.8032 configuration submode. To disable the G.8032 Ethernet ring instance, use the no form of this command.

instance *instance-id*

no instance *instance-id*

Syntax Description

instance-id	Instance ID; currently, supports up to two instances per Ethernet ring. The instance ID can be 1 or 2.

Command Default

None

Command Modes

Ethernet ring G.8032 configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to configure G.8032 Ethernet ring instance:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# instance 1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)#
```

Related Commands

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.
l2vpn, on page 83	Enters L2VPN configuration mode.

interface (VPLS)

To add an interface to a bridge domain that allows packets to be forwarded and received from other interfaces that are part of the same bridge domain, use the **interface** command in L2VPN bridge group bridge domain configuration mode. To remove an interface from a bridge domain, use the **no** form of this command.

interface *type interface-path-id*

no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **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.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **interface** command to enter L2VPN bridge group bridge domain attachment circuit configuration mode. In addition, the **interface** command enters the interface configuration submode to configure parameters specific to the interface.

By default, an interface is not part of a bridge.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the bundle Ethernet interface as an attachment circuit:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/9
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

l2vpn resynchronize forwarding mac-address-table location

To retrieve a MAC address table from network processors and transfer the MAC address tables to the L2FIB manager, use the **l2vpn resynchronize forwarding mac-address-table location** command in EXEC mode.

l2vpn resynchronize forwarding mac-address-table location *node-id*

Syntax Description

node-id	Location of the mac-address-table. The *node-id* argument is entered using the *rack/slot/module* notation.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

To ensure that correct information is displayed, enter this command before issuing any **show** commands for the mac address tables.

The **l2vpn resynchronize forwarding mac-address-table location** command initiates the transfer of MAC learn information from the network processors, to the L2FIB manager. This operation is CPU intensive especially when there are 512K MACs. Therefore, the command is throttled, so that you cannot issue this command back to back. The throttle time depends on the number of MAC addresses. If the number of MAC addresses is under 16K MACs, the throttle time is five seconds. If it is between 16K and 128K, the throttle time is one minute, and if it is between 128K and 256K, the throttle time is two minutes. The throttle time is four minutes for MAC addresses above 256K.

Task ID

Task ID	Operations
l2vpn	read, write, execute

Examples

The following example shows how to retrieve the MAC address table from the network processors:

```
RP/0/RSP0/CPU0:router# l2vpn resynchronize forwarding mac-address-table location 0/4/CPU0
```

Related Commands

Command	Description
show l2vpn forwarding, on page 114	Displays forwarding information from the layer2_fib manager on the line card.

learning disable (VPLS)

To override the MAC learning configuration of a parent bridge or to set the MAC learning configuration of a bridge, use the **learning disable** command in L2VPN bridge group bridge domain MAC configuration mode. To disable this feature, use the **no** form of this command.

learning disable

no learning disable

Syntax Description

This command has no keywords or arguments.

Command Default

By default, learning is enabled on all bridge domains and all interfaces on that bridge inherits this behavior.

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

When set, the **learning disable** command stops all MAC learning either on the specified interface or the bridge domain.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

In the following example, MAC learning is disabled on all ports in the bridge domain called bar, which is applied to all interfaces in the bridge unless the interface has its own MAC learning enable command.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# learning disable
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.

level

To specify the APS message level, use the **level** command in the Ethernet ring G.8032 instance aps-channel configuration submode.

level *number*

Syntax Description

number	The APS message level. The range is from between 0 to 7.

Command Default

None

Command Modes

Ethernet ring G.8032 instance aps-channel configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to enable the G.8032 ring mode:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# instance 1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# description test
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# profile p1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# rpl port0 neighbor
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# inclusion-list vlan-ids e-g
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# aps-channel
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance-aps)# level 3
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

limit (VPLS)

To set the MAC address limit for action, maximum, and notification and to enter L2VPN bridge group bridge domain MAC limit configuration mode, use the **limit** command in L2VPN bridge group bridge domain MAC configuration mode. To remove all limits that were previously configured under the MAC configuration submodes, use the **no** form of this command.

limit

no limit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **limit** command to enter L2VPN bridge group bridge domain MAC limit configuration mode. The **limit** command specifies that one syslog message is sent or a corresponding trap is generated with the MAC limit when the action is violated.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how the MAC limit for the bridge bar is set to 100 with an action of shutdown. After the configuration, the bridge stops all forwarding after 100 MAC addresses are learned. When this happens, a syslog message and an SNMP trap are created.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# limit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# maximum 100
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# action shutdown
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# notification both
```

Related Commands

Command	Description
action (VPLS), on page 142	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 188	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 200	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

mac (VPLS)

To enter L2VPN bridge group bridge domain MAC configuration mode, use the **mac** command in L2VPN bridge group bridge domain configuration mode. To disable all configurations added under the MAC configuration submodes, use the **no** form of this command.

mac

no mac

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enter L2VPN bridge group bridge domain MAC configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)#
```

Related Commands

Command	Description
aging (VPLS), on page 144	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
learning disable (VPLS), on page 178	Overrides the MAC learning configuration of a parent bridge or sets the MAC learning configuration of a bridge.
limit (VPLS), on page 182	Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
static-address (VPLS), on page 262	Adds static entries to the MAC address for filtering.
withdraw (VPLS), on page 273	Disables MAC address withdrawal for a specified bridge domain

mac secure

To configure MAC security at a port and to set the default action that is to be taken when security is violated, use the **mac secure** command in the l2vpn bridge group bridge domain configuration mode. To disable MAC security, use the **no** form of this command.

mac secure {**action** [**none**| **shutdown**| **restrict**]| **logging**| **disable**}

no mac secure {**action** [**none**| **shutdown**]| **logging**| **disable**}

Syntax Description

action	(Optional) Indicates the action to be taken when security is violated.
none	Forwards the violating packet and allows the MAC address to be relearned.
shutdown	Shuts down the violating bridge port.
restrict	Drops the violating packet and disables the learn attempt. **Note** The **restrict** keyword in applicable to interfaces only.
logging	(Optional) Enables logging.
disable	(Optional) Disables mac security.

Command Default

If a MAC address has been learned on a secure port and, a relearn attempt from another port (secure or not) is made, the default action is restrict.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to enable mac security on bridge bar:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#bridge group b1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)#bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#mac secure
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-secure)#
```

This example shows how to shut down a violating bridge port on bridge bar:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#bridge group b1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)#bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#mac secure
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-secure)#action shutdown
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-secure)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

maximum (VPLS)

To configure the specified action when the number of MAC addresses learned on a bridge is reached, use the **maximum** command in L2VPN bridge group bridge domain MAC limit configuration mode. To disable this feature, use the **no** form of this command.

maximum *value*

no maximum *value*

Syntax Description

value	Maximum number of learned MAC addresses. The range is from 5 to 512000.

Command Default

The default maximum value is 4000.

Command Modes

L2VPN bridge group bridge domain MAC limit configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The action can either be flood, no flood, or shutdown. Depending on the configuration, a syslog, an SNMP trap notification, or both are issued.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows when the number of MAC address learned on the bridge reaches 5000 and the bridge stops learning but continues flooding:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# limit
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# maximum 5000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# action no-flood
```

Related Commands

Command	Description
action (VPLS), on page 142	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
limit (VPLS), on page 182	Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
notification (VPLS), on page 200	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

monitor interface (port0)

To specify a port to detect a ring link failure, use the **monitor interface** command in g8032 port0 submode. To delete the port, use the **no** form of this command.

monitor interface *interface-name*

no monitor interface *interface-name*

Syntax Description

interface-name	Name of the monitored interface. The monitored interface must be a sub-interface of the main interface.

Command Default

Configured physical Ethernet or Ether Bundle interface

Command Modes

Ethernet ring g8032 port0 submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows the output from the monitor interface command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# port0 interface TenGigE 0/4/0/0
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port0)# monitor interface GigabitEthernet 0/0/1/0
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port0)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

monitor interface (port1)

To specify the port to detect a ring link failure, use the **monitor interface** command in g8032 port1 submode. To delete the port, use the **no** form of this command.

monitor interface *interface-name*

no monitor interface *interface-name*

Syntax Description

interface-name	Name of the monitored interface. The monitored interface must be a sub-interface of the main interface.

Command Default

Configured physical Ethernet or ether bundle interface

Command Modes

Ethernet ring g8032 port1 submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows the output from the monitor interface command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# port1 interface TenGigE 0/4/0/0
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port1)# monitor interface GigabitEthernet 0/0/1/0
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port1)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

mpls static label (VPLS)

To configure the MPLS static labels and the static labels for the access pseudowire configuration, use the **mpls static label** command in L2VPN bridge group bridge domain VFI pseudowire configuration mode. To assign the dynamic MPLS labels to either the virtual forwarding interface (VFI) pseudowire or the access pseudowire, use the **no** form of this command.

mpls static label local *value value* **remote** *value*

no mpls static label local *value value* **remote** *value*

Syntax Description

local *value*	Configures the local pseudowire label. **Note** Use the **show mpls label range** command to obtain the range for the local labels.
remote *value*	Configures the remote pseudowire label. **Note** The range of values for the remote labels depends on the label allocator of the remote router.

Command Default

By default, the router attempts to assign dynamic labels to the pseudowire.

Command Modes

L2VPN bridge group bridge domain Access/VFI pseudowire configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Ensure that both ends of the pseudowire have matching static labels.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the VFI pseudowire 10.1.1.2 with pseudowire ID of 1000 to use MPLS label 800 and remote MPLS label 500:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi model
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# mpls static label local 800 remote 500
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
neighbor (VPLS), on page 198	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
pw-class , on page 211	Configures the pseudowire class template name to use for the pseudowire.
vfi (VPLS), on page 271	Configures virtual forwarding interface (VFI) parameters.

mtu (VPLS)

To adjust the maximum packet size or maximum transmission unit (MTU) size for the bridge domain, use the **mtu** command in L2VPN bridge group bridge domain configuration mode. To disable this feature, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	MTU size, in bytes. The range is from 46 to 65535.

Command Default

The default MTU value is 1500.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies, but cannot be set smaller than 64 bytes.

The MTU for the bridge domain includes only the payload of the packet. For example, a configured bridge MTU of 1500 allows tagged packets of 1518 bytes (6 bytes DA, 6 bytes SA, 2 bytes ethertype, or 4 bytes qtag).

Note Bridge wide MTU is not enforced on the data traffic.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example specifies an MTU of 1000 bytes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mtu 1000
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
flooding disable, on page 166	Configures flooding for traffic at the bridge domain level or at the bridge port level.
l2vpn, on page 83	Enters L2VPN configuration mode.

neighbor (VPLS)

To add an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI), use the **neighbor** command in the appropriate L2VPN bridge group bridge domain configuration submode. To remove the pseudowire either from the bridge or from the VFI, use the **no** form of this command.

neighbor *A.B.C.D* **pw-id** *value*

no neighbor *A.B.C.D* **pw-id** *value*

Syntax Description

A.B.C.D	IP address of the cross-connect peer.
pw-id *value*	Configures the pseudowire ID and ID value. Range is 1 to 4294967295.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

L2VPN bridge group bridge domain VFI configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **neighbor** command to enter L2VPN bridge group bridge domain VFI pseudowire configuration mode. Alternatively, use the **neighbor** command to enter L2VPN bridge group bridge domain access pseudowire configuration mode.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure an access pseudowire directly under a bridge domain in L2VPN bridge group bridge domain configuration mode:

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)#
```

The following example shows how to configure the parameters for any pseudowire in L2VPN bridge group bridge domain VFI configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 194	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
pw-class , on page 211	Configures the pseudowire class template name to use for the pseudowire.
static-mac-address (VPLS), on page 264	Configures the static MAC address to associate a remote MAC address with a pseudowire or any other bridge interface.
vfi (VPLS), on page 271	Configures virtual forwarding interface (VFI) parameters.

notification (VPLS)

To specify the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit, use the **notification** command in L2VPN bridge group bridge domain MAC limit configuration mode. To use the notification as only a syslog entry, use the **no** form of this command.

notification {**both**| **none**| **trap**}

no notification {**both**| **none**| **trap**}

Syntax Description

both	Sends syslog and trap notifications when the action is violated.
none	Specifies no notification.
trap	Sends trap notifications when the action is violated.

Command Default

By default, only a syslog message is sent when the number of learned MAC addresses reaches the maximum configured.

Command Modes

L2VPN bridge group bridge domain MAC limit configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

A syslog message and an SNMP trap is generated. Alternatively, an SNMP trap is generated. Finally, no notification is generated.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how both a syslog message and an SNMP trap are generated with the bridge bar and learns more MAC addresses than the configured limit:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# limit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# notification both
```

Related Commands

Command	Description
action (VPLS), on page 142	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 188	Configures the specified action when the number of MAC addresses learned on a bridge is reached.

open ring

To specify Ethernet ring g8032 as an open ring, use the **open-ring** command in Ethernet ring g8032 configuration submode. To delete, use the **no** form of this command.

open-ring

no open-ring

This command has no keywords or arguments.

Command Default

The default value is FALSE.

Command Modes

Ethernet ring g8032 configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows the output from the **open-ring** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# open-ring
RP/0/RSP0/CPU0:router(config-l2vpn-erp)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

port0 interface

To enable G.8032 for a specified ring port, use the **port0 interface** command in g8032 configuration port0 submode. To disable, use the **no** form of this command.

port 0 interface *interface name*

no port 0 interface *interface name*

Syntax Description

interface name	Any physical Ethernet or Bundle Ethernet interface. A physical port of the local node connected to G.8032 ring.

Command Default

None

Command Modes

Ethernet ring g8032 configuration port0 submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows the output from the port0 interface command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# port0 interface Bundle-Ether 555
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port0)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

port1

To enable G.8032 for a specified ring port, use the **port1** command in g8032 configuration port1 submode. To disable, use the **no** form of this command.

port1 {**interface** *interface name*| **none**}

Syntax Description

interface *interface name*	Specifies physical Ethernet or Bundle Ethernet interface. A physical port of the local node connected to G.8032 ring. Enables G.8032 for the specified physical port to form a closed ring.
none	Specifies local node endpoint of an open-ring.

Command Default

None

Command Modes

Ethernet ring g8032 configuration port1 submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows the output from the port1 command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# port1 interface TenGigE 0/6/0/3
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port1)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

port-down flush disable (VPLS)

To disable MAC flush when the bridge port is nonfunctional, use the **port-down flush disable** command in the L2VPN bridge group bridge domain MAC configuration mode. Use the **no** form of this command to enable the MAC flush when the bridge port is nonfunctional.

port-down flush disable

no port-down flush disable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

The **port-down flush disable** command disables the MAC flush when the bridge port is nonfunctional.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to disable MAC flush when the bridge port is nonfunctional:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# port-down flush disable
```

Related Commands

Command	Description
action (VPLS), on page 142	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 188	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 200	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

profile

To specify an associated Ethernet ring G.8032 profile, use the **profile** command in the Ethernet ring G.8032 instance configuration submode.

profile *profile-name*

Syntax Description

profile-name	Ethernet ring G.8032 profile name.

Command Default

None

Command Modes

Ethernet ring G.8032 instance configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to specify a G.8032 ring profile name:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# instance 1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# description test
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# profile p1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

pw-class

To configure the pseudowire class template name to use for the pseudowire, use the **pw-class** command in L2VPN bridge group bridge domain Access pseudowire configuration mode. To delete the pseudowire class, use the **no** form of this command.

pw-class *class-name*

no pw-class *class-name*

Syntax Description

class-name	Pseudowire class name.

Command Default

None

Command Modes

L2VPN bridge group bridge domain Access pseudowire configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to attach the pseudowire class to the pseudowire:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# pw-class canada
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 194	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 198	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
vfi (VPLS), on page 271	Configures virtual forwarding interface (VFI) parameters.

pw-oam

To enable the Operations, Administration, and Maintenance (OAM) feature on a pseudowire for defect notifications, use the **pw-oam** command in L2VPN configuration submode. To disable the feature, use the **no** form of this command.

pw-oam refresh transmit *value*

no pw-oam refresh transmit *value*

Syntax Description

refresh transmit	Refresh interval when outbound pseudowire status messages are transmitted.
value	Interval value in seconds. The range is from 1 to 4095. The default value is 30.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to enable the oam feature on a pseudowire:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-oam refresh transmit
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-oam refresh transmit 456
```

Related Commands

Command	Description
pw-class (L2VPN), on page 99	Enters pseudowire class submode to define a pseudowire class template.

route-target

To specify a route target for the VFI, use the **route-target** command in the BGP autodiscovery mode. To return to the default value, use the **no** form of this command.

route-target {*as-number:nn* | *ip-address:nn* **| export | import**}

no route-target {*as-number:nn* | *ip-address:nn* **| export | import**}

Syntax Description

as-number:nn	Autonomous system (AS) number of the route distinguisher. • as-number—16-bit AS number Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535. • nn—32-bit number
ip-address:nn	IP address of the route distinguisher. • ip-address—32-bit IP address • nn—16-bit number
export	Specifies export route target.
import	Specifies import route target.

Command Default

None.

Command Modes

BGP autodiscovery configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure a bridge domain:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EGroup
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain eastdomain
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfieastvfi
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# autodiscovery bgp
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-ad)#route-target 100:20
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

routed

To specify the bridge domain L3 interface, use the **routed** command in L2VPN bridge-group bridge-domain configuration submode. To revert, use the **no** form of the command.

routed interface BVI *BVI interface number*

no routed interface BVI *BVI interface number*

Syntax Description

interface	Bridge domain L3 interface.
BVI	Bridge-Group Virtual Interface.
BVI interface number	BVI interface number. The range is 1-65535.

Command Default

None

Command Modes

L2VPN bridge-group bridge-domain configuration submode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

The example shows how to specify the L3 bridge domain interface:

```
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)# routed interface BVI 100
```

Related Commands

Command	Description
dynamic-arp-inspection, on page 67	Validates Address Resolution Protocol (ARP) packets in a network.
ip-source-guard, on page 73	Enables source IP address filtering on a layer 2 port.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
mtu (VPLS), on page 196	Adjusts the maximum packet size or maximum transmission unit (MTU) size for the bridge domain.
neighbor (VPLS), on page 198	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
pbb, on page 278	Configures the provider backbone bridge core or edge.
shutdown (Bridge Domain), on page 254	Shuts down a bridge domain to bring the bridge and all attachment circuits and pseudowires under it to admin down state.
vfi (VPLS), on page 271	Configures virtual forwarding interface (VFI) parameters.

rpl

To specify one ring port on local node being RPL owner, neighbor or next-neighbor, use the **rpl** command in the Ethernet ring G.8032 instance configuration submode. To disable the port as RPL owner, neighbor or next-neighbor, use the **no** form of this command.

rpl {**port0**| **port1**} {**owner**| **neighbor**| **next-neighbor**}

no rpl {**port0**| **port1**} {**owner**| **neighbor**| **next-neighbor**}

Syntax Description

port0	Assigns port0 as RPL owner, neighbor or next-neighbor.
port1	Assigns port1 as RPL owner, neighbor or next-neighbor.
owner	Assigns port0 or port1 as RPL owner.
neighbor	Assigns port0 or port1 as neighbor.
next-neighbor	Assigns port0 or port1 as next neighbor.

Command Default

None

Command Modes

Ethernet ring G.8032 instance configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to assign port0 as neighbor:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# instance 1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# description test
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# profile p1
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# rpl port0 neighbor
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)#
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show ethernet ring g8032

To display Ethernet ring G.8032 Protection data, use the **show ethernet ring g8032** command in the EXEC mode.

show ethernet ring g.8032 {**brief** *ring-name*| **profile** *ring-profile-name*| **statistics**| **status** {*ring-name*| **location** *location*}| **summary**}

Syntax Description

brief	Displays brief information on the G.8032 ethernet ring.
profile	Displays information about the G.8032 ethernet ring profile.
statistics	Displays the statistics of the G.8032 ethernet ring.
status	Displays the status of the G.8032 ethernet ring.
summary	Displays a summary of the G.8032 ethernet ring.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
vlan	read
interface	read
ethernet-services	read

Examples

This example shows the output of the **show ethernet ring g8032** command:

```
RP/0/RSP0/CPU0:router# show ethernet ring g8032 status


Ethernet ring Subring instance 1 is RPL Owner node in Protection state
  Port0: Bundle-Ether100 (Monitor: Bundle-Ether100)
         APS-Channel: Bundle-Ether100.1
         Status: RPL, faulty, blocked
         Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  Port1: GigabitEthernet0/0/0/38 (Monitor: GigabitEthernet0/0/0/38)
         APS-Channel: GigabitEthernet0/0/0/38.1
         Status: NonRPL
         Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  APS Level: 7
  Open APS ring topology
  Profile: timer-wtr (not defined)
    WTR interval: 5 minutes
    Guard interval: 500 milliseconds
    Hold-off interval: 0 seconds
    Revertive mode

Ethernet ring Subring-2 instance 1 is RPL Owner node in Idle state
  Port0: GigabitEthernet0/0/0/33 (Monitor: GigabitEthernet0/0/0/33)
         APS-Channel: GigabitEthernet0/0/0/33.1
         Status: RPL, blocked
         Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  Port1: GigabitEthernet0/0/0/3 (Monitor: GigabitEthernet0/0/0/3)
         APS-Channel: GigabitEthernet0/0/0/3.1
         Status: NonRPL
         Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  APS Level: 7
  Open APS ring topology
  Profile: timer-wtr (not defined)
    WTR interval: 5 minutes
    Guard interval: 500 milliseconds
    Hold-off interval: 0 seconds
    Revertive mode
RP/0/RSP0/CPU0:router#


RP/0/RSP0/CPU0:router# show ethernet ring g8032 brief
Wed Mar 16 07:14:28.719 UTC

  R: Interface is the RPL-link
  F: Interface is faulty
  B: Interface is blocked
 FS: Local forced switch
 MS: Local manual switch

RingName                         Inst NodeType  NodeState    Port0    Port1
--------------------------------------------------------------------------------
Subring                             1 Owner     Protection   R,F,B
Subring-2                           1 Owner     Idle         R,B
RP/0/RSP0/CPU0:F4-2-A9K#


RP/0/RSP0/CPU0:router# show ethernet ring g8032 summary
Wed Mar 16 07:14:52.419 UTC

Chassis Node Id 0026.982b.c6e7

States
-----------------------------
  Init              0
  Idle              1
  Protection        1
  Manual Switch     0
  Forced Switch     0
  Pending           0
  ---------------------------
  Total             2
RP/0/RSP0/CPU0:router#


RP/0/RSP0/CPU0:router# show ethernet ring g8032 statistics Subring instance 1

Statistics for Ethernet ring Subring instance 1
Local SF detected:
  Port0: 1
  Port1: 0

R-APS   Port0(Tx/Rx)                    Port1(Tx/Rx)
        Last Tx time                    Last Tx time
        Last Rx time                    Last Rx time
--------------------------------------------------------------------------------
NR    : 3/0                             0/0
        Tue Mar 15 04:41:00.964 UTC     Never
        Never                           Never
NR,RB : 0/0                             0/0
        Never                           Never
        Never                           Never
SF    : 19129/0                         19129/0
        Wed Mar 16 07:15:28.995 UTC     Wed Mar 16 07:15:28.774 UTC
        Never                           Never
MS    : 0/0                             0/0
        Never                           Never
        Never                           Never
FS    : 0/0                             0/0
        Never                           Never
        Never                           Never
EVENT : 0/0                             0/0
        Never                           Never
        Never                           Never

State           Last entry into state time
--------------------------------------------------------------------------------
Init          : Tue Mar 15 04:41:00.933 UTC
Idle          : Never
Protection    : Tue Mar 15 04:41:00.973 UTC
Manual Switch : Never
Forced Switch : Never
Pending       : Tue Mar 15 04:41:00.962 UTC
RP/0/RSP0/CPU0:router#


RP/0/RSP0/CPU0:router# show ethernet ring g8032 profile timer-wtr
Wed Mar 16 07:20:04.996 UTC

Ethernet ring profile name: timer-wtr
    WTR interval: 1 minutes
    Guard interval: 500 milliseconds
    Hold-off interval: 0 seconds
    Revertive mode
RP/0/RSP0/CPU0:router#
```

Related Commands

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show l2vpn bridge-domain (VPLS)

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read

Examples

The following sample output shows information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains:

```
RP/0/RSP0/CPU0:router# #show l2vpn bridge-domain
Tue Feb 23 20:21:56.758 PST
Bridge group: 189, bridge-domain: 189, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 2 (2 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/3.189, state: up, Static MAC addresses: 0
    Gi0/1/0/7.189, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
Bridge group: 190, bridge-domain: 190, id: 1, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 0 (0 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
  List of ACs:
  List of Access PWs:
  List of VFIs:
    VFI 190
      Neighbor 10.19.19.19 pw-id 190, state: up, Static MAC addresses: 0
Bridge group: 210, bridge-domain: 210, id: 2, 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: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/7.210, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI 210
      Neighbor 10.19.19.19 pw-id 210, state: up, Static MAC addresses: 0
Bridge group: 211, bridge-domain: 211, id: 3, 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: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/7.211, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI 211
      Neighbor 10.19.19.19 pw-id 211, state: up, Static MAC addresses: 0
Bridge group: 215, bridge-domain: 215, id: 4, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 2 (2 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/3.215, state: up, Static MAC addresses: 0
    Gi0/1/0/7.215, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI 215
      Neighbor 10.19.19.19 pw-id 215, state: up, Static MAC addresses: 0
Bridge group: 2130, bridge-domain: 2130, id: 5, 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: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/7.2130, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI 2130
      Neighbor 10.19.19.19 pw-id 2130, state: up, Static MAC addresses: 0
```

This table describes the significant fields shown in the display.

Table 5: show l2vpn bridge-domain Command Field Descriptions

Field	Description
Bridge group	Name of bridge domain group is displayed.
bridge-domain	Name of bridge domain is displayed.
id	ID assigned to this bridge domain is displayed.
state	Current state of the bridge domain is displayed.
ShgId	ID for the default Split Horizon Group assigned to all attachment circuits and access pseudowires that are part of this bridge domain is displayed. **Note** Members of the special Split Horizon Group ID 0 forwards to other members of the same SPG.

The following example shows sample output for a bridge named bd1:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain bd-name bd1
```

```
Bridge group: g1, bridge-domain: bd1, 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: 1 (1 up)
  List of ACs:
    Gi0/1/0/0, state: up, Static MAC addresses: 2, MSTi: 0 (unprotected)
  List of Access PWs:
  List of VFIs:
    VFI 1
      Neighbor 10.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
```

The following sample output shows brief information about the bridges:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain brief
Bridge Group/Bridge-Domain Name  ID    State      Num ACs/up     Num PWs/up
-------------------------------- ----- ---------- -------------- ------------
bg1/bd1                          0     up         1/1            0/0
bg1/bd2                          1     up         0/0            0/0
bg1/bd3                          2     up         0/0            0/0
```

This table describes the significant fields shown in the display.

Table 6: show l2vpn bridge-domain brief Command Field Descriptions

Field	Description
Bridge Group/Bridge-Domain Name	Bridge domain group name followed by the bridge domain name are displayed.
ID	ID assigned to this bridge domain is displayed.
State	Current state of the bridge domain is displayed.
Num ACs/up	Total number of attachment circuits that are up in this bridge domain is displayed.
Num PWs/up	Total number of pseudowires that are up in this bridge domain is displayed. The count includes both VFI pseudowires and access pseudowires.

The following sample output shows detailed information:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain detail

Bridge group: 210, bridge-domain: 210, id: 2, state: up, ShgId: 0, MSTi: 0
  MAC learning: enabled
  MAC withdraw: 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
  Security: disabled
  Split Horizon Group: none
  DHCPv4 snooping: disabled
  IGMP Snooping profile: none
  Bridge MTU: 9000
  Filter MAC addresses:
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
  List of ACs:
    AC: GigabitEthernet0/1/0/7.210, state is up
```

```
      Type VLAN; Num Ranges: 1
     vlan ranges: [100, 100]
      MTU 9008; XC ID 0x440007; interworking none; MSTi 0 (unprotected)
      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
      Security: disabled
      Split Horizon Group: enabled
      DHCPv4 snooping: disabled
      IGMP Snooping profile: none
      Storm Control: disabled
      Static MAC addresses:
      Statistics:
        packet totals: receive 31645, send 6
        byte totals: receive 2405020, send 456
        Storm control drop counters:
          packet totals: broadcast 0, multicast 0, unknown unicast 0
          byte totals: broadcast 0, multicast 0, unknown unicast 0
  List of Access PWs:
  List of VFIs:
    VFI 210
      PW: neighbor 10.19.19.19, PW ID 210, state is up ( established )
        PW class not set, XC ID 0xfffc0004
        Encapsulation MPLS, protocol LDP
        PW type Ethernet, control word disabled, interworking none
        PW backup disable delay 0 sec
        Sequencing not set
                MPLS         Local                          Remote
          ------------ ------------------------------ -------------------------
          Label        16001                          16
          Group ID     0x2                            0x0
          Interface    210                            unknown
          MTU          9000                           9000
          Control word disabled                       disabled
          PW type      Ethernet                       Ethernet
          VCCV CV type 0x2                            0x2
                         (LSP ping verification)        (LSP ping verification)
          VCCV CC type 0x6                          0x2
                       (router alert label)           (router alert label)
                       (TTL expiry)
          ------------ ------------------------------ -------------------------
        Create time: 13/04/1900 14:36:13 (17:46:22 ago)
        Last time status changed: 13/04/1900 15:37:03 (16:45:32 ago)
        MAC withdraw message: send 0 receive 0
        Static MAC addresses:
        Statistics:
          packet totals: receive 6, send 31655
          byte totals: receive 432, send 2279160
      IGMP Snooping profile: none
      VFI Statistics:
        drops: illegal VLAN 0, illegal length 0
```

The following sample output shows detailed information including P2MP enabled, P-Tree-ID and LSM ID with 1 VFI PW in a bridge domain:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain detail

Bridge group: bg1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw for Access PW: enabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4294967295, 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 profile: none
  Bridge MTU: 1500
  MIB cvplsConfigIndex: 1
  Filter MAC addresses:
  Create time: 27/04/2011 10:00:47 (00:14:31 ago)
  No status change since creation
  ACs: 0 (0 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
  List of Access PWs:
  List of VFIs:
    VFI 1
      P2MP:
        RSVP-TE transport, BGP signaling, PTree ID 14
        LSM-ID: 0xdeadbeef
      PW: neighbor 110.110.110.110, PW ID 1234, state is up (established)
        PW class not set, XC ID 0xfffc0001
        Encapsulation MPLS, protocol LDP
        Source address 100.100.100.100
        PW type Ethernet, control word disabled, interworking none
        PW backup disable delay 0 sec
        Sequencing not set

        PW Status TLV in use
          MPLS         Local                          Remote
       ------------ ------------------------------ -------------------------
          Label        16000                          16000
          Group ID     0x0                            0x0
          Interface    1                              1
          MTU          1500                           1500
          Control word disabled                       disabled
          PW type      Ethernet                       Ethernet
          VCCV CV type 0x2                            0x2
                       (LSP ping verification)        (LSP ping verification)
          VCCV CC type 0x6                            0x6
                       (router alert label)           (router alert label)
                       (TTL expiry)                   (TTL expiry)
          ------------ ------------------------------ -------------------------
        Incoming Status (PW Status TLV):
          Status code: 0x0 (Up) in Notification message
        Outgoing Status (PW Status TLV):
          Status code: 0x0 (Up) in Notification message
        MIB cpwVcIndex: 4294705153
        Create time: 27/04/2011 10:14:45 (00:00:34 ago)
        Last time status changed: 27/04/2011 10:15:16 (00:00:02 ago)
        MAC withdraw message: send 0 receive 0
        P2MP-PW:
          FEC            Local                         Remote
          -------------- ----------------------------- ----------------------
          Label          NULL (inclusive tree)         NULL (inclusive tree)
          P2MP ID        1                             1
          Flags          0x00                          0x00
          PTree Type     RSVP-TE                       RSVP-TE
          Tunnel ID      1000                          1000
          Ext. Tunnel ID 192.168.0.1                   192.168.0.2
          -------------- ----------------------------- ----------------------
          P2MP forwarding: enabled
        Static MAC addresses:
        Statistics:
          packets: received 0, sent 0
          bytes: received 0, sent 0
      DHCPv4 snooping: disabled
      IGMP Snooping profile: none
      VPN-ID: 1
      VFI Statistics:
        drops: illegal VLAN 0, illegal length 0
```

The following sample output shows that when a bridge operates in VPWS mode, the irrelevant information for MAC learning is suppressed:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain detail
Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  MAC learning: enabled
  MAC withdraw: 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: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
  List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      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: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146
  List of Access PWs:
  List of VFIs:
    VFI 1
      PW: neighbor 1.1.1.1, PW ID 1, state is up ( established )
        PW class mpls, XC ID 0xff000001
        Encapsulation MPLS, protocol LDP
        PW type Ethernet, control word disabled, interworking none
        PW backup disable delay 0 sec
        Sequencing not set
                MPLS         Local                          Remote
          ------------ ------------------------------ ----------
          Label        16003                          16003
          Group ID     0x0                            0x0
          Interface    1                              1
          MTU          1500                           1500
          Control word disabled                       disabled
          PW type      Ethernet                       Ethernet
          VCCV CV type 0x2                            0x2
                       (LSP ping verification)        (LSP ping verification)
          VCCV CC type 0x2                            0x2
                       (router alert label)           (router alert label)
          ------------ ------------------------------ ----------
        Create time: 12/03/2008 14:03:00 (17:17:30 ago)
        Last time status changed: 13/03/2008 05:57:58 (01:22:31 ago)
        MAC withdraw message: send 0 receive 0
        Static MAC addresses:
        Statistics:
          packet totals: receive 3918814, send 3918024
          byte totals: receive 305667492, send 321277968
      VFI Statistics:
        drops: illegal VLAN 0, illegal length 0

Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-edge, I-SID: 1234
  Core-bridge: pbb-bd2
  MAC learning: enabled
  MAC withdraw: 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: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
List of PBBs:
    PBB Edge, state is up
      XC ID 0x2000001
      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: yes
      Split Horizon Group: none
      DHCPv4 snooping: disabled
      IGMP Snooping profile:
      Storm Control: disabled
      Unknown-unicast-bmac: 666.777.888
      CMAC to BMAC Mapping Table:
         CMAC             |    BMAC
         -------------------------------------------------
         222.333.444     |    777.888.999
         333.444.555     |    888.999.111
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146

 List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      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: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146


Bridge group: g2, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-core
  Number of associated pbb-edge BDs: 1
  MAC learning: enabled
  MAC withdraw: 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: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
```

```
ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
List of PBBs:
    PBB Core, state is up
      Vlan-id: 1; XC ID 0x2000001
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 600, Action: none, Notification: syslog
      MAC limit reached: no
      Security: disabled
      Split Horizon Group: none
      DHCPv4 snooping: profile foo
      IGMP Snooping profile:
      Storm Control: disabled

List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      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: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146
```

This table describes the significant fields shown in the display.

Table 7: show l2vpn bridge-domain detail Command Field Descriptions

Field	Description
Bridge group	Name of bridge domain group is displayed.
bridge-domain	Name of bridge domain is displayed.
ID	ID assigned to this bridge domain is displayed.
state	Current state of the bridge domain is displayed.
ShgId	Split horizon group ID. This field is not used.
MSTi	ID for the Multiple Spanning Tree.

Field	Description
Split Horizon Group	Shows whether the AC is a member of the split horizon group for ACs. There is only one split horizon group for ACs per bridge domain. • Enabled—The port belongs to the split horizon group for ACs. • None—The port does not belong to the split horizon group for ACs.

The following sample output shows filter information about the bridge-domain group named g1:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain group g1

Bridge group: g1, bridge-domain: bd1, 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: 1 (1 up)
  List of ACs:
    Gi0/1/0/0, state: up, Static MAC addresses: 2, MSTi: 0 (unprotected)
  List of Access PWs:
  List of VFIs:
    VFI 1
      Neighbor 10.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
```

The following sample output shows display the filter information for the interface on the bridge domain:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain interface gigabitEthernet 0/1/0/0

Bridge group: g1, bridge-domain: bd1, 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: 1 (1 up)
  List of ACs:
    Gi0/1/0/0, state: up, Static MAC addresses: 2, MSTi: 0 (unprotected)
```

The following sample output shows that the bridge domain contains the pseudowires to match the filter for the neighbor:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain neighbor 10.1.1.1

Bridge group: g1, bridge-domain: bd1, 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: 1 (1 up)
  List of Access PWs:
  List of VFIs:
    VFI 1
      Neighbor 10.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
```

The following sample output shows the summary information for the bridge domain including number of bridge-domains with P2MP PW enabled:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain summary

Number of groups: 1, bridge-domains: 1, Up: 1, Shutdown: 0
Default: 1, pbb-edge: 0, pbb-core: 0
Bridge-domains with P2MP PW enabled: 1
Number of ACs: 3 Up: 3, Down: 0
Number of PWs: 2 Up: 2, Down: 0, Standby: 0
```

This table describes the significant fields shown in the display.

Table 8: show l2vpn bridge-domain summary Command Field Descriptions

Field	Description
Number of groups	Number of configured bridge domain groups is displayed.
bridge-domains	Number of configured bridge domains is displayed.
Shutdown	Number of bridge domains that are in Shutdown state is displayed.
Number of ACs	Number of attachment circuits that are in Up state and Down state are displayed.
Number of PWs	Number of pseudowires that are in Up state and Down state are displayed. This includes the VFI pseudowire and the access pseudowire.

This example shows the sample output of a configured flow label:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain detail
Bridge group: g1, bridge-domain: d1, id: 0, state: up, ShgId: 0, MSTi: 0
 ......
  PW: neighbor 3.3.3.3, PW ID 2, state is up ( established )
    PW class class1, XC ID 0x1000002
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word disabled, interworking none
    PW backup disable delay 0 sec
  Sequencing not set
    Flow label flags configured (Rx=1,Tx=1), negotiated (Rx=0,Tx=1)
```

Related Commands

Command	Description
clear l2vpn bridge-domain (VPLS), on page 154	Clears the MAC addresses and restarts the bridge domains on the router.

show l2vpn ethernet ring g8032

To display an overview of the G.8032 ethernet ring configuration, use the **show l2vpn ethernet ring g8032** command in EXEC mode.

show l2vpn ethernet ring g8032 *[name]* [**brief**| **detail**| **instance** *ID*| **private**]

Syntax Description

name	Ethernet ring G.8032 name.
brief	Brief information about the G.8032 ethernet ring configuration.
detail	Information in detail about the G.8032 ethernet ring configuration.
instance*ID*	Instance number 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 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read

Examples

This example shows the output from the **show l2vpn ethernet ring g8032** command:

```
# show l2vpn ethernet ring g8032 foo instance 1
Ethernet ring g8032 foo
  Port0: GigabitEthernet0/1/2/0
  Port1: GigabitEthernet0/1/2/1
  Instance 1
     Inclusion-list vlan ids: 500-1000, 1017
     aps-channel
        port0: GigabitEthernet0/1/2/0.1
        port1: GigabitEthernet0/1/2/1.1


# show l2vpn ethernet ring g8032 foo instance 1 brief
Ring      instance  status
--------- --------  --------
Foo        1        resolved

# show l2vpn ethernet ring g8032 foo instance 1 detail
Ethernet ring g8032 foo
  Operating in Provider Bridge mode
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Exclusion-list vlan ids: 2000-2100, untagged
  Open-ring: no

  Instance 1
     Description: This_is_a_sample
     Profile    : none
     RPL        : none
     Inclusion-list vlan ids: 500-1000, 1017
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.1
        port1: GigabitEthernet0/1/2/1.1


# show l2vpn ethernet ring g8032 foo instance 1 private
Ethernet ring g8032 foo (task-id = cisco-support)
  Operating in Provider Bridge mode
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Exclusion-list vlan ids: 2000-2100, untagged
  Open-ring: no

  Instance 1
     Description: This_is_a_sample
     Profile    : none
     RPL        : none
     Inclusion-list vlan ids: 500-1000, 1017
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.1
        port1: GigabitEthernet0/1/2/1.1


   ethernet ring g8032 trace history [Num events: 6]
   ---------------------------------------------------
   Time                Event                     Sticky Many
   ====                =====                     ====== ====
   05/18/2010 21:45:54 Create                    No     No
   05/18/2010 21:45:54 Resolved                  No     No
   05/18/2010 21:45:57 Create                    No     No
   05/18/2010 21:45:57 Modify                    No     No
   05/18/2010 21:45:57 Resolved                  No     No
   05/18/2010 21:45:57 Delete                    No     No
```

Related Commands

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show l2vpn forwarding bridge-domain (VPLS)

To display information on the bridge that is used by the forwarding layer, use the **show l2vpn forwarding bridge-domain** command in EXEC mode.

show l2vpn forwarding bridge-domain [*bridge-domain-name*] {**detail**| **hardware** {**egress**| **ingress**}} **location** *node-id*

Syntax Description

bridge-domain-name	(Optional) Name of a bridge domain.
detail	Displays all the detailed information on the attachment circuits and pseudowires.
hardware	Displays the hardware location entry.
egress	Reads information from the egress PSE.
ingress	Reads information from the ingress PSE.
location *node-id*	Displays the bridge-domain information for the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

For each bridge, you can display summary information about the number of bridge ports, number of MAC addresses, and so forth.

The **detail** keyword displays detailed information on the attachment circuits and pseudowires, and is meant for field investigation by a specialized Cisco engineer.

Note All bridge ports in the bridge domain on that line card are displayed. Therefore, if the bridge domain contains non-local bridge ports, those are displayed as well.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following sample output shows bridge-domain information for location 0/1/CPU0:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain location 0/1/CPU0

Bridge-Domain Name               ID     Ports addr   Flooding Learning State
-------------------------------- ------ ----- ------ -------- -------- ---------
g1:bd1

Bridge-domain name: g1:bd1, id: 0, state: up
 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: yes
 Security: disabled
 DHCPv4 snooping: profile not known on this node
 Bridge MTU: 1500 bytes
 Number of bridge ports: 2
 Number of MAC addresses: 65536
 Multi-spanning tree instance: 0

  GigabitEthernet0/1/0/0, state: oper up
    Number of MAC: 32770
    Sent(Packets/Bytes): 0/21838568
    Received(Packets/Bytes): 5704781/444972918

  Nbor 1.1.1.1 pw-id 1
    Number of MAC: 32766
    Sent(Packets/Bytes): 0/0
    Received(Packets/Bytes): 5703987/444910986
            0      2     65536  Enabled  Enabled  UP
```

The following sample output shows detailed information for hardware location 0/1/CPU0 from the egress pse:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain hardware egress detail location
 0/1/CPU0

Bridge-domain name: g1:bd1, id: 0, state: up
 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: yes
 Security: disabled
 DHCPv4 snooping: profile not known on this node
 Bridge MTU: 1500 bytes
 Number of bridge ports: 2
 Number of MAC addresses: 65536
 Multi-spanning tree instance: 0
```

This table describes the significant fields shown in the display:

Table 9: show l2vpn forwarding bridge-domain Command Field Descriptions

Field	Description
Bridge-Domain Name	Name of bridge domain is displayed.
Bridge ID	ID assigned to this bridge domain is displayed.
Ports	Number of ports that are part of this bridge domain is displayed.
MAC Addr	Number of MAC addresses that are learned on this bridge domain is displayed.
Flooding	Flooding of packets are displayed if they are enabled on this bridge domain.
Learning	Learning of MAC addresses are displayed if they are enabled on this bridge domain.
State	Current state of the bridge domain is displayed.

The following sample output shows detailed information with P2MP PW enabled on the bridge domain:

```
RP/0/RSP0/CPU0:router#  show l2vpn forwarding bridge-domain detail location
Tue May 24 23:14:22.934 EDT

Bridge-domain name: bg1:bd1, id: 0, state: up
 MAC learning: enabled
 MAC port down flush: 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 Secure: disabled, Logging: disabled
 DHCPv4 snooping: profile not known on this node
 Dynamic ARP Inspection: disabled, Logging: disabled
 IP Source Guard: disabled, Logging: disabled
 IGMP snooping: disabled, flooding: enabled
 Bridge MTU: 1500 bytes
 Number of bridge ports: 1
 Number of MAC addresses: 0
 Multi-spanning tree instance: 0
 P2MP PW RSVP-TE enabled, LSM ID: 0x12

  GigabitEthernet0/0/0/2.3, state: oper up
    Number of MAC: 0
  Nbor 2.2.2.2 pw-id 101, state: oper up
    Number of MAC: 0
```

Related Commands

Command	Description
clear l2vpn bridge-domain (VPLS), on page 154	Clears the MAC addresses and restarts the bridge domains on the router.

show l2vpn forwarding bridge-domain mac-address (VPLS)

To display the summary information for the MAC address, use the **show l2vpn forwarding bridge-domain mac-address** command in EXEC mode.

show l2vpn forwarding bridge-domain [*bridge-domain-name*] **mac-address** {*MAC-address*| **detail**| **hardware** {**egress**| **ingress**}| **interface** *type interface-path-id*| **neighbor** *address* **pw-id** *pw-id*} **location** *node-id*

Syntax Description

bridge-domain-name	(Optional) Name of a bridge domain.
MAC-address	MAC address.
detail	Displays detailed information for the MAC address.
hardware	Reads information from the hardware.
egress	Reads information from the egress PSE.
ingress	Reads information from the ingress PSE.
interface	Displays the match for the attachment circuit subinterface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
neighbor *address*	Displays the match for the neighbor IP address.
pw-id *pw-id*	Displays the match for the pseudowire ID.
location *node-id*	Displays the bridge-domain information for the MAC address of the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	This command was introduced.
Release 3.7.2	This command was introduced.
Release 3.8.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

The following sample output shows the specified location of the bridge-domain name g1:bd1 for the MAC address:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 location 0/1/CPU0
                                 Bridge       MAC
Bridge-Domain Name               ID     Ports addr   Flooding Learning State
-------------------------------- ------ ----- ------ -------- -------- ---------
g1:bd1                           0      2     65536  Enabled  Enabled  UP
```

The following sample output shows the list of MAC addresses that are learned on a specified bridge and summary information for the addresses:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
-------------------------------------------------------------------------------
0000.0000.0000 static  Gi0/1/0/0                   N/A        N/A
0000.0001.0101 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0102 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0103 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0104 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0105 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0106 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0107 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0108 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0109 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010a dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010b dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010c dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010d dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010e dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010f dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0110 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0111 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0112 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
....
```

The following sample output shows the MAC address on a specified interface on a specified bridge:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 mac-address 1.2.3 location
 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
--------------------------------------------------------------------------------
0001.0002.0003 static  Gi0/1/0/0                   N/A        N/A
```

The following sample output shows the hardware information from the egress pse:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 mac-address hardware
egress location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
--------------------------------------------------------------------------------
0000.0000.0000 static  Gi0/1/0/0                   N/A        N/A
0000.0001.0101 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0102 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0103 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0104 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0105 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0106 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0107 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0108 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0109 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.010a dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.010b dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.010c dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.010d dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.010e dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.010f dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0110 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0111 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0112 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0113 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
0000.0001.0114 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 24s
...
```

The following sample output shows the MAC addresses that are learned on a specified pseudowire on a specified bridge:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address neighbor 10.1.1.1
pw-id 1 location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
--------------------------------------------------------------------------------
0000.0003.0101 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0102 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0103 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0104 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0105 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0106 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0107 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0108 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0109 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010a dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010b dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010c dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010d dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010e dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010f dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0110 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0111 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0112 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0113 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0114 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0115 dynamic 10.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
...
```

The following sample output shows the detailed information for MAC addresses that are learned on a specified interface and on specified bridge of a specified interface card. The sample output lists all the MAC addresses, the learned location, and the current age.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 mac-address interface
gigabitEthernet 0/1/0/0 location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
-------------------------------------------------------------------------------
0000.0000.0000 static  Gi0/1/0/0                   N/A        N/A
0000.0001.0101 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0102 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0103 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0104 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0105 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0106 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0107 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0108 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0109 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.010a dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.010b dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.010c dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.010d dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.010e dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.010f dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0110 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0111 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0112 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0113 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
0000.0001.0114 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 14s
```

The following example shows the list of MAC addresses along with the location details:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address detail location
0/7/CPU0
l2fib_edm_fill_mac_bag mac_info 0 l2fm_l3_encap_vlan=0
l2fib_get_mac_l3_encap_vlan_str
l2fib_edm_fill_mac_bag mac_info 0 l2fm_l3_encap_vlan=0
l2fib_get_mac_l3_encap_vlan_str
Bridge-domain name: bg1:bd1, id: 0, state: up
 MAC learning: enabled
 MAC port down flush: 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 Secure: disabled, Logging: disabled
 DHCPv4 snooping: profile not known on this node
 Dynamic ARP Inspection: disabled, Logging: disabled
 IP Source Guard: disabled, Logging: disabled
 IGMP snooping: disabled, flooding: enabled
 Routed interface: BVI100, Xconnect id: 0xfff00001, state: up
  IRB platform data: {0x0, 0x0, 0x0, 0x0}, len: 4
 Bridge MTU: 1500 bytes
 Number of bridge ports: 1
 Number of MAC addresses: 2
 Multi-spanning tree instance: 0

 Mac Address: 029d.af84.4105, LC learned: N/A
   Age: N/A, Flag: static, BVI
   L3 encapsulation Vlan = 0

 GigabitEthernet0/0/0/0.1, state: oper up
    Number of MAC: 1

 Mac Address: 0000.0002.0003, LC learned: N/A
   Age: N/A, Flag: static
```

```
      L3 encapsulation Vlan = 1001

RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
--------------------------------------------------------------------------------
0000.0000.0000 static  Gi0/1/0/0                   N/A        N/A
0000.0001.0101 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0102 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0103 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0104 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0105 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0106 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0107 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0108 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0109 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010a dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010b dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010c dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010d dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010e dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.010f dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0110 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0111 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
0000.0001.0112 dynamic Gi0/1/0/0                   0/1/CPU0   0d 0h 2m 22s
....
```

Related Commands

Command	Description
show l2vpn forwarding bridge-domain (VPLS), on page 237	Displays information on the bridge that is used by the forwarding layer.

show l2vpn forwarding ethernet ring g8032

To display an overview of the G.8032 ethernet ring configuration from L2Forwarding Information Base (L2FIB) process, use the **show l2vpn forwarding ethernet ring g8032** command in EXEC mode.

show l2vpn forwarding ethernet ring g8032 *name* [**detail**| **instance** *ID*| **location**| **private**]

Syntax Description

name	Ethernet ring G.8032 name.
detail	Information in detail about the G.8032 ethernet ring configuration.
instance*ID*	Instance number about the G.8032 ethernet ring configuration.
location	Location specified in the rack/slot/module notation.
private	Private information about the G.8032 ethernet ring configuration.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read

Examples

This example shows the output from the **show l2vpn forwarding ethernet ring g8032** command:

```
# show l2vpn forwarding ethernet ring g8032 private location <r/s/i>
Ethernet ring g8032 foo (task-id = cisco-support)
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Open-ring: no
  TCN propagation: no
  Instance 1
     Profile    : none
     RPL        : none
     aps-channel
        port0: GigabitEthernet0/1/2/0.1, status: bound
        port1: GigabitEthernet0/1/2/1.1, status: unbound
  Instance 2
     Profile    : none
     RPL        : none
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.10, status: unbound
   ethernet ring g8032 trace history [Num events: 6]
   ---------------------------------------------------
   Time                Event                     Sticky Many
   ====                =====                     ====== ====
   05/18/2010 21:45:54 Create                    No     No
   05/18/2010 21:45:57 Create                    No     No
   05/18/2010 21:45:57 Modify                    No     No
   05/18/2010 21:45:57 Delete                    No     No

# show l2vpn forwarding ethernet ring g8032 foo instance 1 detail location <r/s/i>
Ethernet ring g8032 foo
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Open-ring: no
  TCN propagation: no
  Instance 1
     Profile    : none
     RPL        : none
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.1, status: bound
        port1: GigabitEthernet0/1/2/1.1, status: unbound

# show l2vpn forwarding ethernet ring g8032 foo instance 1 private location <r/s/i>
Ethernet ring g8032 foo (task-id = cisco-support)
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Open-ring: no
  TCN propagation: no
  Instance 1
     Profile    : none
     RPL        : none
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.1, status: bound
        port1: GigabitEthernet0/1/2/1.1, status: unbound

   ethernet ring g8032 instance trace history [Num events: 6]
   ----------------------------------------------------------
   Time                Event                     Sticky Many
   ====                =====                     ====== ====
   05/18/2010 21:45:54 Create                    No     No
   05/18/2010 21:45:57 Create                    No     No
   05/18/2010 21:45:57 Modify                    No     No
   05/18/2010 21:45:57 Delete                    No     No
```

Related Commands

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show l2vpn forwarding protection main-interface

To display an overview of the main interface or instance operational information from L2Forwarding Information Base (L2FIB), use the **show l2vpn forwarding protection main-interface** command in EXEC mode.

show l2vpn forwarding protection main-interface [*interface name*] [**detail**| **location**| **private**]

Syntax Description

interface name	Interface name of the Ethernet ring G.8032 name.
detail	Information in detail about the G.8032 ethernet ring configuration.
location	Brief information 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 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read

Examples

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

```
# show l2vpn forwarding protection main-interface location <r/s/i>
```

```
Main Interface ID                Instance   State
-------------------------------- -------------- --------
GigabitEthernet0/0/0/0           1          forward
GigabitEthernet0/0/0/0           2          forward
GigabitEthernet0/0/0/1           1          forward


# show l2vpn forwarding protection main-interface detail location <r/s/i>
Main Interface ID                Instance  State    # of subIntf
-------------------------------- --------  -------- -------------
GigabitEthernet0/0/0/0           1        forward   1
GigabitEthernet0/0/0/0           2        forward    3
GigabitEthernet0/0/0/1           1        forward    1


# show l2vpn forwarding protection main-interface private location <r/s/i>

Main Interface ID                Instance State    # of subIntf
-------------------------------- -------- -------- ------------
GigabitEthernet0/0/0/0           1       forward   1

   Base info: version=0xaabbcc1c, flags=0x0, type=14, reserved=0
   Ifhandle: 0x20000040, cfg_instance: 1, Protected: no
```

Related Commands

Command	Description
l2vpn, on page 83	Enters L2VPN configuration mode.

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 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read

Examples

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: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, on page 83	Enters L2VPN configuration mode.

shutdown (Bridge Domain)

To shut down a bridge domain to bring the bridge and all attachment circuits and pseudowires under it to admin down state, use the **shutdown** command in L2VPN bridge group bridge domain configuration mode. To re-enable the bridge domain, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

By default, the bridge is not shutdown.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

When a bridge domain is disabled, all VFIs associated with the bridge domain are disabled. You can still attach or detach members to or from the bridge domain as well as the VFIs associated with the bridge domain.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to disable the bridge domain named bar:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# shutdown
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

shutdown (VFI)

To disable virtual forwarding interface (VFI), use the **shutdown** command in L2VPN bridge group bridge domain VFI configuration mode. To re-enable VFI, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

By default, the VFI is not shutdown.

Command Modes

L2VPN bridge group bridge domain VFI configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to disable VFI:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# shutdown
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 194	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 198	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).

signaling-protocol

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

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

no signaling-protocol {**bgp**| **ldp**}

Syntax Description

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

Command Default

LDP signaling is enabled.

Command Modes

BGP autodiscovery configuration

L2VPN bridge group bridge domain VFI multicast P2MP configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable signaling for BGP protocol:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EGroup
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain eastdomain
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi eastvfi
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# autodiscovery bgp
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-ad)#route-target 100:20
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-ad)#signaling-protocol bgp
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

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. To remove the AC from the group, use the **no** form of this command.

split-horizon group

no 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 3.7.2	This command was introduced.

Usage Guidelines

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

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 adds an EFP under a GigabitEthernet interface to the AC split horizon group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group metroA
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain east
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet0/1/0/6.15
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# split-horizon group
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# commit
```

Related Commands

Command	Description
show l2vpn bridge-domain (VPLS), on page 224	Display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains.

static-address (VPLS)

To add static entries to the MAC address for filtering, use the **static-address** command in L2VPN bridge group bridge domain MAC configuration mode. To remove entries profiled by the combination of a specified entry information, use the **no** form of this command.

static-address *MAC-address* **drop**

no static-address *MAC-address* **drop**

Syntax Description

MAC-address	Static MAC address that is used to filter on the bridge domain.
drop	Drops all traffic that is going to the configured MAC address.

Command Default

No static MAC address is configured.

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add static MAC entries in L2VPN bridge group bridge domain MAC configuration mode. This entry causes all packets with destination MAC address 1.1.1 to be dropped.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# static-address 1.1.1 drop
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.

static-mac-address (VPLS)

To configure the static MAC address to associate a remote MAC address with a pseudowire or any other bridge interface, use the **static-mac-address** command in the appropriate L2VPN bridge group bridge domain configuration submode. To disable this feature, use the **no** form of this command.

static-mac-address *MAC-address*

no static-mac-address *MAC-address*

Syntax Description

MAC-address	Static address to add to the MAC address.

Command Default

None

Command Modes

L2VPN bridge group bridge domain VFI pseudowire configuration

L2VPN bridge group bridge domain attachment circuit configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to associate a remote MAC address with a pseudowire:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi model
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# static-mac-address 1.1.1
```

The following example shows how to associate a GigabitEthernet interface from a bridge domain to static MAC address 1.1.1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# static-mac-address 1.1.1
```

The following example shows how to associate an access pseudowire to static MAC address 2.2.2:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# neighbor 10.1.1.2 pw-id 2000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)# static-mac-address 2.2.2
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 194	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 198	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
vfi (VPLS), on page 271	Configures virtual forwarding interface (VFI) parameters.

tcn-propagation

To enable topology change notification (TCN) propagation, use the **tcn-propagation** command in the L2VPN configuration submode.

tcn-propagation

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Examples

This example shows how to enable the G.8032 ring mode:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# tcn-propagation
RP/0/RSP0/CPU0:router(config-l2vpn)#
```

Related Commands

Command	Description
ethernet ring g8032, on page 160	Enables G.8032 ring mode and enters the G.8032 configuration submode.

time (VPLS)

To configure the maximum aging time, use the **time** command in L2VPN bridge group bridge domain MAC aging configuration mode. To disable this feature, use the **no** form of this command.

time *seconds*

no time *seconds*

Syntax Description

seconds	MAC address table entry maximum age. The range is from 300 to 30000 seconds. Aging time is counted from the last time that the switch saw the MAC address. The default value is 300 seconds.

Command Default

seconds: 300

Command Modes

L2VPN bridge group bridge domain MAC aging configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

If no packets are received from the MAC address for the duration of the maximum aging time, the dynamic MAC entry previously learned is removed from the forwarding table.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to increase the maximum aging time to 600 seconds. After 600 seconds of inactivity from a MAC address, the MAC address is removed form the forwarding table.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# time 600
```

Related Commands

Command	Description
aging (VPLS), on page 144	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
type (VPLS), on page 269	Configures the type for MAC address aging.

type (VPLS)

To configure the type for MAC address aging, use the **type** command in L2VPN bridge group bridge domain MAC aging configuration mode. To disable this feature, use the **no** form of this command.

type {**absolute| inactivity**}

no type {**absolute| inactivity**}

Syntax Description

absolute	Configures the absolute aging type.
inactivity	Configures the inactivity aging type.

Command Default

By default, the inactivity type is configured.

Command Modes

L2VPN bridge group bridge domain MAC aging configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

In general, the type is set to inactivity. With an inactivity type configuration, a MAC address is removed from the forwarding table after the MAC address is inactive for the configured aging time.

With an absolute type configuration, a MAC address is always removed from the forwarding table after the aging time has elapsed once it is initially learned.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the MAC address aging type to absolute for every member of the bridge domain named bar:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
```

```
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# type absolute
```

Related Commands

Command	Description
aging (VPLS), on page 144	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.
time (VPLS), on page 267	Configures the maximum aging time.

vfi (VPLS)

To configure virtual forwarding interface (VFI) parameters and to enter L2VPN bridge group bridge domain VFI configuration mode, use the **vfi** command in L2VPN bridge group bridge domain configuration mode. To remove all configurations that are made under the specified VFI, use the **no** form of this command.

vfi *vfi-name*

no vfi *vfi-name*

Syntax Description

vfi-name	Name of the specified virtual forwarding interface.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to create a VFI:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 194	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 198	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).

withdraw (VPLS)

To disable MAC address withdrawal for a specified bridge domain, use the **withdraw** command in L2VPN bridge group bridge domain MAC configuration mode. To enable this feature, use the **no** form of this command

withdraw {**access-pw disable** | **disable**}

no withdraw {**access-pw disable** | **disable** }

Syntax Description

access-pw disable	Disables the sending of MAC withdraw messages to access pseudowires.
disable	Disables MAC address withdrawal.

Command Default

By default, MAC address withdrawal is enabled.

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.0.0	The **access-pw disable** keyword was added.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable disable MAC withdrawal:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# withdraw disable
```

The following example shows how to disable sending MAC withdrawal messages to access pseudowires:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# withdraw access-pw disable
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
mac (VPLS), on page 184	Enters L2VPN bridge group bridge domain MAC configuration mode.

Provider Backbone Bridge Commands

The IEEE 802.1ah standard (Ref [4]) provides a means for interconnecting multiple provider bridged networks inorder to build a large scale end-to-end Layer 2 provider bridged network.

For detailed information about PBB concepts, configuration tasks, and examples, see the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

backbone-source-mac

To configure the backbone source MAC address, use the **backbone-source-mac** command in pbb configuration mode. To return to the default behavior, use the **no** form of this command.

Note If the backbone source MAC address is not configured then one of the reserved addresses from the Chassis MAC pool is chosen automatically. To view the reserved address, use the **show l2vpn pbb backbone-source-mac** command.

backbone-source-mac *mac-address*

no backbone-source-mac *mac-address*

Syntax Description

mac address	Backbone source MAC address in hexadecimal format.

Command Default

None

Command Modes

PBB configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

In the following example, the backbone source MAC address is set to 0045.1200.04:

```
config
l2vpn
  pbb
    backbone-source-mac 0045.1200.0400
  !
!
```

Related Commands

Command	Description
pbb, on page 278	Configures the provider backbone bridge core or edge.

pbb

To configure the provider backbone bridge core or edge, use the **pbb** command in the bridge domain configuration submode. To return to the default behavior, use the **no** form of this command.

pbb {**edge i-sid** *service-id* **core-bridge** *core-bridge-domain-name*| **core**}

no pbb {**edge i-sid** *service-id* **core-bridge** *core-bridge-domain-name*| **core**}

Syntax Description

edge	Configures the PBB edge.
i-sid	Specifies the service instance identifier. The ranges is from 256 to 16777214. **Note** The 16777215 (0xFFFFFF) service instance identifier is reserved for wildcard.
service-id	Service instance identifier.
core-bridge	Specifies the name of the core-bridge domain connected to that edge-bridge domain.
core-bridge-domain-name	Core bridge domain name.
core	Configures the PBB core.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

This command allows you to enter pbb edge configuration mode or pbb core configuration mode.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the PBB edge component:

```
config
l2vpn
  bridge group PBB
    bridge-domain PBB-EDGE
      interface GigabitEthernet0/0/0/38.100
      !
      interface GigabitEthernet0/2/0/30.150
      !
      pbb edge i-sid 1000 core-bridge PBB-CORE
   !
 !
!
```

The following example shows how to configure the PBB core component:

```
config
l2vpn
 bridge group PBB
  bridge-domain PBB-CORE
   interface G0/5/0/10.100
   !
   interface G0/2/0/20.200
   !
   pbb core
  !
 !
!
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.

rewrite ingress tag push

To configure the backbone VLAN ID for a PBB core bridge, use the **rewrite ingress tag push** command in the PBB core configuration mode. To return to the default behavior, use the **no** form of this command.

rewrite ingress tag push dot1ad *vlan-id* **symmetric**

Syntax Description

dot1ad	Indicates that the IEEE 802.1ad provider bridges encapsulation type is used.
vlan-id	VLAN ID. Range is from 1 to 4094.
symmetric	Specifies that all rewrites must be symmetric.

Command Default

None

Command Modes

PBB core configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the backbone VLAN ID for the PBB core bridge:

```
config
l2vpn
  bridge group PBB
    bridge-domain PBB-CORE
      interface G0/5/0/10.100
      !
      interface G0/2/0/20.200
      !
      pbb core
       rewrite ingress tag push dot1ad 100 symmetric
  !
 !
!
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
pbb, on page 278	Configures the provider backbone bridge core or edge.

static-mac-address

To map a customer destination MAC address to backbone destination MAC address, use the **static-mac-address** command in the PBB edge configuration mode. To return to the default behavior, use the **no** form of this command.

static-mac-address *cust-mac-address* **bmac** *bmac-mac-address*

no static-mac-address *cust-mac-address* **bmac** *bmac-mac-address*

Syntax Description

cust-mac-address	Customer destination MAC address in hexadecimal format.
bmac	Specifies that the static backbone MAC address must be mapped with the customer MAC address.
bmac-mac-address	Static backbone MAC address in hexadecimal format.

Command Default

None

Command Modes

PBB edge configuration mode

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to map the customer MAC address with the backbone MAC address:

```
interface GigabitEthernet0/0/0/0.1 l2transport  encapsulation dot1q 10 !
interface GigabitEthernet0/0/0/0.2 l2transport  encapsulation dot1q 2 !
interface GigabitEthernet0/0/0/1
 shutdown
!
```

```
interface GigabitEthernet0/0/0/2
 shutdown
!
interface GigabitEthernet0/0/0/3
 shutdown
!
interface GigabitEthernet0/0/0/4
 shutdown
!
l2vpn
 bridge group bg12
  bridge-domain bd1
   interface GigabitEthernet0/0/0/0.1
    static-mac-address 0002.0003.0004
   !
   interface GigabitEthernet0/0/0/0.2
   !
   pbb edge i-sid 1000 core-bridge bd2
    static-mac-address 0006.0007.0008 bmac 0004.0005.0006
   !
  !
 !
!
end
!
```

The following example shows the output of the **show l2vpn bridge-domain** command:

```
##sh l2vpn bridge-domain m mac-address  mroute

Mac Address    Type    Learned from/    LC learned     Mapped to
       Filtered on    Resync Age
-------------------------------------------------------------------------------------------
0002.0003.0004 static  Gi0/0/0/0.1                 N/A         N/A    N/A
0006.0007.0008 static  BD id: 0                    N/A         N/A  0004.0005.0006
```

Note To resynchronize the MAC table from the network processors, use the **l2vpn resynchronize forwarding mac-address-table location** *<r/s/i>* command.

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
pbb, on page 278	Configures the provider backbone bridge core or edge.
l2vpn, on page 83	Enters L2VPN configuration mode.

unknown-unicast-bmac

To configure the unknown unicast backbone MAC address for a PBB edge bridge, use the **unknown-unicast-bmac** command in the PBB edge configuration mode. To return to the default behavior, use the **no** form of this command.

unknown-unicast-bmac *mac-address*

no unknown-unicast-bmac *mac-address*

Syntax Description

mac-address	Unknown unicast backbone MAC address in hexadecimal format.

Command Default

None

Command Modes

PBB edge configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the unknown unicast backbone MAC address for a PBB edge bridge:

```
config
l2vpn
  bridge group PBB
    bridge-domain PBB-EDGE
      interface GigabitEthernet0/0/0/38.100
      !
      interface GigabitEthernet0/2/0/30.150
      !
      pbb edge i-sid 1000 core-bridge PBB-CORE
        unknown-unicast-bmac 0123.8888.8888
      !
    !
  !
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 150	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 152	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 83	Enters L2VPN configuration mode.
pbb, on page 278	Configures the provider backbone bridge core or edge.

show l2vpn bridge-domain pbb

To display the provider backbone bridge details, use the **show l2vpn bridge-domain pbb** command in EXEC mode.

show l2vpn bridge-domain pbb {**core** [**brief**| **detail**| **hardware**| **private**]| **edge** [**brief**| **core-bridge**| **detail**| **hardware**| **private**]| **i-sid** *service-id* [**brief**| **detail**| **hardware**| **private**]}

Syntax Description

core	Displays the PBB core.
edge	Displays the PBB edge.
i-sid	Displays the service instance identifier.
service-id	Service ID.
brief	Displays brief information about the PBB core, edge or service instance identifier.
detail	Displays detailed information about the PBB core, edge or service instance identifier.
hardware	Displays hardware information.
private	Displays private information about the PBB core, edge or service instance identifier.
core-bridge	Displays the name of the core-bridge domain connected to the edge-bridge domain.

Command Default

None

Command Modes

l2vpn

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

The following examples shows the output from the **show l2vpn bridge-domain pbb** command:

Example 1:

```
#show l2vpn bridge-domain isid 1234
Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-edge, I-SID: 1234
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
List of PBBs:
    PBB Edge, state: up, Static MAC addresses: 0
    List of ACs:
    Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0
```

Example 2:

```
#show l2vpn bridge-domain detail isid 1234
Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-edge, I-SID: 1234
  Core-bridge: pbb-bd2
  MAC learning: enabled
  MAC withdraw: 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: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
 List of PBBs:
    PBB Edge, state is up
      XC ID 0x2000001
      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: yes
      Split Horizon Group: none
      DHCPv4 snooping: disabled
      IGMP Snooping profile:
      Storm Control: disabled
      Unknown-unicast-bmac: 666.777.888
      CMAC to BMAC Mapping Table:
         CMAC             |    BMAC
         -------------------------------------------------
         222.333.444     |    777.888.999
         333.444.555     |    888.999.111
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146

  List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
```

```
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      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: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146
```

Example 3:

```
#show l2vpn bridge-domain pbb edge
Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-edge, I-SID: 1234
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
List of PBBs:
    PBB Edge, state: up, Static MAC addresses: 2
List of ACs:
    Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0

Bridge group: g2, bridge-domain: pbb-bd3, id: 3, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-edge, I-SID: 2345
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
List of PBBs:
     EDGE, state: up, Static MAC addresses: 2
List of ACs:
    Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0


Bridge group: g2, bridge-domain: pbb-bd4, id: 4, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-edge, I-SID: 3456
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
List of PBBs:
     PBB Edge, state: up, Static MAC addresses: 2
List of ACs:
    Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0
```

Example 4:

```
#show l2vpn bridge-domain pbb-edge detail
Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-edge, I-SID: 1234
  Core-bridge: pbb-bd2
  MAC learning: enabled
  MAC withdraw: 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: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
  ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up
  List of PBBs:
    PBB Edge, state is up
```

```
      XC ID 0x2000001
      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: yes
      Split Horizon Group: none
      DHCPv4 snooping: disabled
      IGMP Snooping profile:
      Storm Control: disabled
      Unknown-unicast-bmac: 666.777.888

      CMAC to BMAC Mapping Table:
         CMAC             |    BMAC
         -------------------------------------------------
         222.333.444     |    777.888.999
         333.444.555     |    888.999.111
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146

  List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      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: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146
```

Example 5:

```
#show l2vpn bridge-domain pbb-core
Bridge group: g2, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-core
  Number of associated pbb-edge BDs: 1
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up
  List of PBBs:
    PBB Core, state: up
  List of ACs:
    Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0
```

Example 6

```
#show l2vpn bridge-domain pbb-core detail
Bridge group: g2, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-core
  Number of associated pbb-edge BDs: 1
  MAC learning: enabled
  MAC withdraw: 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: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
ACs: 1 (1 up), PBB: 1
List of PBBs:
    PBB Core, state is up
      Vlan-id: 1; XC ID 0x2000001
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 600, Action: none, Notification: syslog
      MAC limit reached: no
      Security: disabled
      Split Horizon Group: none
      DHCPv4 snooping: profile foo
      IGMP Snooping profile:
      Storm Control: disabled
  List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      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: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146
```

Example 7:

```
#show l2vpn bridge-domain pbb-edge core-bridge core-bd brief
Bridge Group/????????????????????? ID    State      Num ACs/up     Num PWs/up
Bridge-Domain Name
--------------------------------------------- ------ ------- ---------------------
bg/pbb-bd1 ??????????????????????????1      up           0/0 ?????????0/0
bg/pbb-bd2 ??????????????????????????2      up           0/0 ?????????0/0
bg/pbb-bd3 ??????????????????????????3      up           0/0 ?????????0/0


RP/0/0/CPU0:ios#show l2vpn bridge-domain pbb edge core-bridge bd
Bridge group: bg, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Type: pbb-edge, I-SID: 4001
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 0 (0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
  List of PBBs:
    PBB Edge, state: up, Static MAC addresses: 2
   …

Bridge group: bg, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
  Type: pbb-edge, I-SID: 4002
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 0 (0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
  List of PBBs:
    PBB Edge, state: up, Static MAC addresses: 1
  …

Bridge group: bg, bridge-domain: pbb-bd3, id: 3, state: up, ShgId: 0, MSTi: 0
  Type: pbb-edge, I-SID: 4003
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 0 (0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
```

```
List of PBBs:
  PBB Edge, state: up, Static MAC addresses: 0
…
```

Related Commands

Command	Description
pbb, on page 278	Configures the provider backbone bridge core or edge.

show l2vpn forwarding bridge pbb

To display the PBB bridge forwarding information, use the **show l2vpn forwarding bridge pbb** command in EXEC mode.

show l2vpn forwarding bridge pbb core [**debug**| **detail**| **hardware**| **location**| **private**]| **edge** [**core-bridge**| **debug**| **detail**| **hardware**| **location**| **private**]| **i-sid** *service-id* [**debug**| **detail**| **hardware**| **location**| **private**]

Syntax Description

debug	Displays the debug information.
core	Displays the PBB core.
edge	Displays the PBB edge.
i-sid *service-id*	Displays the service instance identifier.
brief	Displays brief information about the PBB core, edge or service instance identifier.
detail	Displays detailed information about the PBB core, edge or service instance identifier.
hardware	Displays hardware information.
private	Displays private information about the PBB core, edge or service instance identifier.
core-bridge	Displays the name of the core-bridge domain connected to the edge-bridge domain.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows the output from the **show l2vpn forwarding pbb backbone-source-mac** command:

```
#show l2vpn forwarding backbone-source-mac location 0/1/CPU0
333.444.555
```

Related Commands

Command	Description
pbb, on page 278	Configures the provider backbone bridge core or edge.

show l2vpn forwarding pbb backbone-source-mac

To display the provider backbone source MAC forwarding information, use the **show l2vpn forwarding pbb backbone-source-mac** command in EXEC mode.

show l2vpn forwarding pbb backbone-source-mac {**debug** [**detail**| **location**| **private**]| **detail** [**debug**| **location** *node-id*]| **location** *node-id*| **private**}

Syntax Description

debug	Displays the debug information.
detail	Displays the detailed PBB forwarding information.
location	Specifies the location.
node-id	Node ID.
private	Displays private information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows the output from the **show l2vpn forwarding pbb backbone-source-mac** command:

```
#show l2vpn forwarding backbone-source-mac location 0/1/CPU0
333.444.555
```

Related Commands

Command	Description
pbb, on page 278	Configures the provider backbone bridge core or edge.

show l2vpn pbb backbone-source-mac

To display the provider backbone source MAC information, use the **show l2vpn pbb backbone-source-mac** command in EXEC mode.

show l2vpn pbb backbone-source-mac

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows the output from the **show l2vpn pbb backbone-source-mac** command:

```
#show l2vpn pbb backbone-source-mac
0111.0222.0333
```

Related Commands

Command	Description
pbb, on page 278	Configures the provider backbone bridge core or edge.

Multiple Spanning Tree Protocol Commands

For detailed information about MSTP concepts, configuration tasks, and examples, see the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

bridge-id

To set the bridge ID for this device for an Access Gateway instance, use the **bridge-id** command in MSTAG interface configuration, REPAG Interface configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

bridge-id *id* [**startup-value** *startup-id*]

Syntax Description

id	MAC address of the switch. It can be any 48-bit value.
startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-id	Sets the startup bridge ID.

Command Default

For MSTAG/REPAG, the MAC address of the switch. For PVSTAG/PVRSTAG, the interface MAC address.

If no startup value is specified, the normal value is used during startup.

Command Modes

MSTAG interface configuration, REPAG Interface configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG VLAN configuration and PVRSTAG VLAN configuration submodes.

Usage Guidelines

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

When configuring access gateway, this command is used to modify the value of the bridge ID that is advertised in the STP BPDUs.

Task ID

Task ID	Operations
interface (for MSTAG/REPAG)	read, write
ethernet-services (for PVSTAG/PVRSTAG)	read, write

Examples

The following example shows how to set the bridge ID:

```
RP/0/RSP0/CPU0:router(config-mstag-if)# bridge-id 001c.0000.0011
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

bringup delay

To configure a delay when an interface is first created before it is added to the MSTP topology, use the **bringup delay** command in the MSTP configuration mode.

bringup delay for *interval* {**seconds**| **minutes**| **hours**}

no bringup delay for *interval* {**seconds**| **minutes**| **hours**}

Syntax Description

interval	Length of time to delay adding the interface to the MSTP topology.
seconds	Specifies the delay in seconds.
minutes	Specifies the delay in minutes.
hours	Specifies the delay in hours.

Command Default

If no bringup delay is configured, interfaces are added to the MSTP topology as soon as they are created.

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

This command is used to change the behaviour of MSTP when interfaces are first functional (for example, when a line card boots for the first time). By default, interfaces are added to the MSTP topology, and may be placed in the forwarding state, as soon as the system declares that the interfaces are functional. However, at this point the data plane may not be fully prepared to forward traffic on the interface. If a bringup delay is configured, MSTP keeps the interface in blocked state for the specified delay, and adds it to the MSTP topology only after the specified interval has occurred.

For information on configuring bringup delay, refer to the *Implementing Multiple Spanning Tree Protocol* module of the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure the bringup delay:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#spanning-tree mst A
RP/0/RSP0/CPU0:router(config-mstp)# bringup delay for 20 seconds
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

clear ethernet mvrp statistics

To clear MVRP statistics for ethernet interfaces, use the **clear ethernet mvrp statistics** command in the EXEC mode.

clear ethernet mvrp statistics {**interface** *type interface-path-id*| **location** *location*| **all**}

Syntax Description

interface	(Optional) Clears the MVRP statistics for the given interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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	Clears MVRP statistics for interfaces in a particular location.
location	Specifies the fully qualified location.
all	Clears the MVRP statistics for all interfaces.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to configure the bringup delay:

```
RP/0/RSP0/CPU0:router# clear ethernet mvrp statistics all
```

Related Commands

Command	Description
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.

cost

To set the internal path cost for a given instance on the current port, use the **cost** command in MSTAG interface instance or REPAG interface instance configuration submode.

cost *cost* [**startup-value** *startup-cost*]

Syntax Description

cost	Port cost. Range is 1 to 200000000.
startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-id	Sets the startup internal path cost.

Command Default

If the startup value is not specified, it defaults to 200000000.

Command Modes

MSTAG interface instance configuration, REPAG Instance Configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

This command is used when configuring Access Gateway, to change the cost value that is advertised for this MSTI in the STP BPDUs.

Note MSTP cost for bundle interfaces is fixed to 10000 and does not depend on the number of interfaces and the speed of individual members.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the port cost to 10000:

```
RP/0/RSP0/CPU0:router(config-mstag-if-inst)# cost 10000
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
instance (MSTAG/REPAG), on page 344	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

debug ethernet mvrp packets

To enable debugging of sent and received MVRP packets, use the **debug ethernet mvrp packets** command in the EXEC mode. To disable debugging, use the **no** form of this command.

debug ethernet mvrp packets {**brief**| **full**| **hexdump**} [**direction** {**received**| **sent**}] [**interface** *interface-name*| **location** *node-id*]

no debug ethernet mvrp packets {**brief**| **full**| **hexdump**} [**direction** {**received**| **sent**}] [**interface** *interface-name*| **location** *node-id*]

Syntax Description

brief	Enables brief debugging output.
full	Enables full debugging output.
hexdump	Enables full debugging output along with the raw contexts of the packet in hex.
direction	{Optional} Restricts output to a packet direction.
received	Indicates packets received.
sent	Indicates packets sent.
interface *interface-name*	{Optional} Filters by interface. Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Indicates the location. The *node-id* argument is entered in the rack/slot/module notation.

Command Default

By default, debugging is enabled for both directions for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to enable debugging of brief MVRP packets:

```
RP/0/RSP0/CPU0:router#debug ethernet mvrp packets brief
Thu Oct 28 02:56:35.048 DST
```

The following example shows how to enable debugging of full MVRP packets on a specific location:

```
RP/0/RSP0/CPU0:router#debug ethernet mvrp packets full location 0/0/CPU0
Mon Nov 15 20:02:13.636 PST
```

The following example shows how to enable debugging of brief MVRP packets received at a specific interface:

```
RP/0/RSP0/CPU0:router#debug ethernet mvrp packets brief direction received interface
gigabitEthernet 0/0/0/1
Thu Nov 25 21:09:01.986 PST
```

Related Commands

Command	Description
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.

debug ethernet mvrp protocol

To enable MVRP protocol debugging on a specific interface, location or vlan, use the **debug ethernet mvrp protocol** command in the EXEC mode. To disable debugging, use the **no** form of this command.

debug ethernet mvrp protocol [**vlan** *vlan-id*] [**interface** *interface-name*| **location** *node-id*]

no debug ethernet mvrp protocol [**vlan** *vlan-id*] [**interface** *interface-name*| **location** *node-id*]

Syntax Description

vlan *vlan-id*	{Optional} Specific vlan-id to filter on.
interface *interface-name*	{Optional} Filters by interface. Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Indicates the location. The *node-id* argument is entered in the rack/slot/module notation.

Command Default

By default, debug is enabled for all vlans, interfaces, and locations.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to debug an ethernet mvrp protocol:

```
RP/0/RSP0/CPU0:router#debug ethernet mvrp protocol
Thu Oct 28 03:05:21.575 DST

RP/0/RSP0/CPU0:router#debug ethernet mvrp protocol location 0/0/CPU0
Mon Nov 15 20:11:56.607 PST

RP/0/RSP0/CPU0:router#debug ethernet mvrp protocol interface gigabitEthernet 0/0/0/1
Mon Nov 15 20:12:49.776 PST
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.

debug spanning-tree mst packet

To enable debugging for sent and received MSTP packets, use the **debug spanning-tree mst packet** command in the EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree mst packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

no debug spanning-tree mst packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

Syntax Description

brief	Enables brief debugging output.
full	Enables full debugging output.
sent	Display packets being sent.
received	Display packets being received.
interface *interface-name*	{Optional} Filters by interface. Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If an interface is not specified, then debug is enabled for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to enable brief debugging for received packets:

```
RP/0/RSP0/CPU0:router#debug spanning-tree mst packet brief received
Mon Nov 15 20:42:58.584 PST
```

The following example shows how to enable brief debugging for received packets at a specific location:

```
RP/0/RSP0/CPU0:router#debug spanning-tree mst packet brief received location 0/0/CPU0

Mon Nov 15 20:44:15.082 PST
```

The following example shows how to enable brief debugging for received packets on a specific interface:

```
RP/0/RSP0/CPU0:router#debug spanning-tree mst packet brief received interface gigabitEthernet
 0/0/0/1
Mon Nov 15 20:45:40.047 PST
```

Related Commands

Command	Description
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
debug spanning-tree packet raw, on page 318	Enables debugging raw packet output for all received packets or sent packets.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

debug spanning-tree mst protocol-state

To enable debugging protocol-state changes such as port role or state changes, topology change notification, use the **debug spanning-tree mst protocol-state** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree mst protocol-state [**instance** *instance-id*] [**interface** *interface-name*]

no debug spanning-tree mst protocol-state [**instance** *instance-id*] [**interface** *interface-name*]

Syntax Description

instance *instance-id*	View debug for a specific MSTI.
interface *interface-name*	View debug for a specific interface.

Command Default

If no instance or interface is specified, debug is enabled for all instances and interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to enable protocol state debugging:

```
RP/0/RSP0/CPU0:router#debug spanning-tree mst protocol-state
Mon Nov 15 20:53:52.793 PST

RP/0/RSP0/CPU0:router#debug spanning-tree mst protocol-state interface gigabitEthernet
0/0/0/1
Mon Nov 15 20:54:57.310 PST

RP/0/RSP0/CPU0:router#debug spanning-tree mst protocol-state instance 4094
Mon Nov 15 20:59:35.860 PST
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

debug spanning-tree mstag packet

To enable MSTAG packet debugging, use the **debug spanning-tree mstag packet** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree mstag packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

no debug spanning-tree mstag packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

Syntax Description

brief	Enables brief debugging output.
full	Enables full debugging output.
received	Display packets being received.
sent	Display packets being sent.
interface *interface-name*	{Optional} Filters by interface. Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If the interface is not specified, the debug is enabled for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to enable MSTAG packet debugging:

```
RP/0/RSP0/CPU0:router#debug spanning-tree mstag packet brief received
Mon Nov 15 21:11:30.464 PST

RP/0/RSP0/CPU0:router#debug spanning-tree mstag packet full sent interface gigabitEthernet
 0/0/0/1
Mon Nov 15 21:12:23.391 PST
```

Related Commands

Command	Description
debug spanning-tree packet raw, on page 318	Enables debugging raw packet output for all received packets or sent packets.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.

debug spanning-tree packet raw

To enable debugging raw packet output for all received packets or sent packets, use the **debug spanning-tree packet raw** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree packet raw {**sent**| **received**} [**interface** *interface-name*]

no debug spanning-tree packet raw {**sent**| **received**} [**interface** *interface-name*]

Syntax Description

received	Display packets being received.
sent	Display packets being sent.
interface *interface-name*	{Optional} Filters by interface. Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If an interface is not specified, debug is enabled for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

This command enables raw packet debug for all STP protocols: MSTP, MSTAG, REPAG, PVSTAG and PVRSTAG.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to enable debugging raw packet output for packets received at a specific location:

```
RP/0/RSP0/CPU0:router#debug spanning-tree packet raw received location 0/0/CPU0
Mon Nov 15 21:16:42.570 PST
```

The following example shows how to enable debugging raw packet output for packets sent from a specific interface:

```
RP/0/RSP0/CPU0:router#debug spanning-tree packet raw sent interface gigabitEthernet 0/0/0/1
Mon Nov 15 21:17:43.303 PST
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.

debug spanning-tree pvrstag packet

To enable packet debugging for sent and received PVRSTAG packets, use the **debug spanning-tree pvrstag packet** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree pvrstag packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

no debug spanning-tree pvrstag packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

Syntax Description

brief	Enables brief debugging output.
full	Enables full debugging output.
sent	Indicates packets sent.
received	Indicates packets received.
interface *interface-name*	{Optional} Filters by interface. Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If an interface is not specified, then debug is enabled for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	debug

Examples

The following example shows how to enable packet debugging for PVRSTAG packets received at a specific interface:

```
RP/0/RSP0/CPU0:router#debug spanning-tree pvrstag packet brief received interface
gigabitEthernet 0/0/0/1
Wed Nov 24 22:12:33.861 PST
```

The following example shows how to enable packet debugging for PVRSTAG packets sent from a specific interface:

```
RP/0/RSP0/CPU0:router#debug spanning-tree pvrstag packet brief sent interface gigabitEthernet
 0/0/0/1
Wed Nov 24 22:15:12.893 PST
```

Related Commands

Command	Description
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.

debug spanning-tree pvstag packet

To enable packet debugging for sent and received PVSTAG packets, use the **debug spanning-tree pvstag packet** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree pvstag packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

no debug spanning-tree pvstag packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

Syntax Description

brief	Enables brief debugging output.
full	Enables full debugging output.
sent	Indicates packets sent.
received	Indicates packets received.
interface *interface-name*	{Optional} Filters by interface. Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If an interface is not specified, then debug is enabled for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	debug

Examples

The following example shows how to enable packet debugging for PVSTAG packets received at a specific interface:

```
RP/0/RSP0/CPU0:router#debug spanning-tree pvstag packet brief received interface
gigabitEthernet 0/0/0/1
Wed Nov 24 22:12:33.861 PST
```

The following example shows how to enable packet debugging for PVSTAG packets sent from a specific interface:

```
RP/0/RSP0/CPU0:router#debug spanning-tree pvstag packet brief sent interface gigabitEthernet
 0/0/0/1
Wed Nov 24 22:15:12.893 PST
```

Related Commands

Command	Description
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.

debug spanning-tree repag packet

To enable Resilient Ethernet Protocol (REP) Access Gateway debugging commands, use the **debug spanning-tree repag packet** command in the EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree repag packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

no debug spanning-tree repag packet {**brief**| **full**} {**sent**| **received**} [**interface** *interface-name*]

Syntax Description

brief	Enables brief debugging output.
full	Enables full debugging output.
received	Display packets being received.
sent	Display packets being sent.
interface *interface-name*	{Optional} Filters by interface. Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If an interface is not specified, then debug is enabled for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how to enable brief debug for REP Access Gateway packets received at a specified interface.

```
RP/0/RSP0/CPU0:router#debug spanning-tree repag packet brief received interface
gigabitEthernet 0/0/0/1
Mon Nov 15 21:26:08.155 PST
```

The following example shows how to enable full debug for REP Access Gateway packets sent from a specific location:

```
RP/0/RSP0/CPU0:router#debug spanning-tree repag packet full sent location 0/0/CPU0
Mon Nov 15 21:27:10.674 PST
```

edge-mode

To enable MSTAG edge mode for Multiple Spanning Tree Instance (MSTI), use the **edge-mode** command in MSTAG instance configuration submode. Use the **no** form of this command to disable the MSTAG edge mode.

edge-mode

no edge-mode

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

MSTAG instance configuration mode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ethernet-services	read, write

Examples

This example shows the output from the **edge-mode** command:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#spanning-tree mstag A
RP/0/RSP0/CPU0:router(config-mstag)#interface GigabitEthernet 0/2/0/1.1
RP/0/RSP0/CPU0:router(config-mstag-if)#instance 100
RP/0/RSP0/CPU0:router(config-mstag-if-inst)#edge-mode
RP/0/RSP0/CPU0:router(config-mstag-if-inst)#
```

Related Commands

Command	Description
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.

Command	Description
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.

external-cost (MSTAG/REPAG)

To set the external path cost on the current port, use the **external-cost** command in MSTAG interface or REPAG interface configuration submode.

external-cost *cost* [**startup-value** *startup-cost*]

Syntax Description

cost	Interface external path cost. Range is 1 to 200000000.
startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-cost	Sets the external path cost.

Command Default

If no startup-value is configured, the startup value defaults to 200000000.

Command Modes

MSTAG interface configuration, REPAG Interface Configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

This command is used when configuring Access Gateway, to change the external cost that it advertised in STP BPDUs sent from this interface.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the external cost to 10000:

```
RP/0/RSP0/CPU0:router(config-mstag-if)# external-cost 10000
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

external-cost (MSTP)

To set the external path cost on the current port, use the **external-cost** command in MSTP interface configuration submode.

external-cost *cost*

Syntax Description

cost	Port cost. Range is 1 to 200000000.

Command Default

The default path cost depends on the speed of the link.

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the external cost to 10000:

```
RP/0/RSP0/CPU0:router:router(config-mstp-if)# external-cost 10000
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

flush containment disable

To disable the flush containment feature on a bridge, use the **flush containment disable** command in the MSTP configuration submode.

flush containment disable

Syntax Description

This command has no keywords or arguments.

Command Default

Flush containment feature is enabled.

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Flush containment is a Cisco feature that helps prevent unnecessary MAC flushes. Refer to the *Implementing Multiple Spanning Tree Protocol* module in the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to disable the flush containment feature on a bridge:

```
RP/0/RSP0/CPU0:router(config-mstp)# flush containment disable
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

forward-delay

To set the forward-delay parameter for the bridge, use the **forward-delay** command in MSTP configuration submode.

forward-delay *seconds*

Syntax Description

seconds	Bridge forward delay time in seconds. Range is 4 to 30.

Command Default

seconds: 15

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the forward-delay parameter for the bridge to 20:

```
RP/0/RSP0/CPU0:router(config-mstp)# forward-delay 20
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

Command	Description
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

guard root

To prevent a port from becoming the root port for the switch, use the **guard root** command in MSTP interface configuration submode.

guard root

Syntax Description

This command has no keywords or arguments.

Command Default

RootGuard is disabled.

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

This command enables the Root Guard feature on the interface, by preventing the port from becoming a root port. This feature can be used to enforce the location of the root bridge within the MSTP network. For more information on guard root feature, refer to the *Implementing Multiple Spanning Tree Protocol* module in the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enable RootGuard on the port:

```
RP/0/RSP0/CPU0:router(config-mstp-if)# guard root
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.

Command	Description
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

guard topology-change

To enable topology change guard on the port, use the **guard topology-change** command in MSTP interface configuration submode.

guard topology-change

Syntax Description

This command has no keywords or arguments.

Command Default

TopologyChangeGuard is disabled.

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

This command enables topology change guard (also known as restricted TCN) on this interface. When this feature is enabled, topology changes originating at this interfaces, or received in BPDUs on this interface, are not propagated to the rest of the MSTP network. For more information on guard topology, refer to the *Implementing Multiple Spanning Tree Protocol* module in the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enable TopologyChangeGuard on the port:

```
RP/0/RSP0/CPU0:router(config-mstp-if)# guard topology-change
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.

Command	Description
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

hello-time (Access Gateway)

To configure the frequency of sending BPDUs on this interface, use the **hello-time** command in MSTAG interface configuration, REPAG Interface configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

hello-time *seconds*

Syntax Description

seconds	Hello time in seconds. Range is 1 to 2.

Command Default

seconds: 2

Command Modes

MSTAG interface configuration, REPAG Interface configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG VLAN configuration and PVRSTAG VLAN configuration mode.

Usage Guidelines

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

Task ID

Task ID	Operations
interface (for MSTAG/REPAG)	read, write
ethernet-services (for PVSTAG/PVRSTAG)	read, write

Examples

The following example shows how to set the port hello time to 1:

```
RP/0/RSP0/CPU0:router(config-mstag-if)# hello-time 1
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

hello-time (MSTP)

To set the port hello time, use the **hello-time** command in MSTP interface configuration submode.

hello-time *seconds*

Syntax Description

seconds	Hello time in seconds. Range is 1 to 2.

Command Default

seconds: 2

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the port hello time to 1:

```
RP/0/RSP0/CPU0:router(config-mstp-if)# hello-time 1
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

instance (MSTAG/REPAG)

To enter MSTAG Instance configuration mode or REPAG Instance configuration mode, use the **instance** command in MSTAG Interface or REPAG Interface configuration mode respectively.

instance *id*

Syntax Description

id	MSTI ID. Range is 0 to 4094.

Command Default

None

Command Modes

MST AG interface configuration, REPAG interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter MSTAG Instance configuration submode:

```
RP/0/RSP0/CPU0:router(config-mstag)# instance 101
RP/0/RSP0/CPU0:router(config-mstag-inst)#
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

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 3.7.1	This command was introduced.

Usage Guidelines

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

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:

```
RP/0/RSP0/CPU0:router(config-mstp)# instance 101
RP/0/RSP0/CPU0:router(config-mstp-inst)#
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.

Command	Description
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
priority (MSTP), on page 389	Sets the bridge priority for the current MSTI
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
vlan-id (MSTP), on page 461	Associates a set of VLAN IDs with the current MSTI.

instance cost

To set the internal path cost for a given instance on the current port, use the **instance cost** command in MSTP interface configuration submode.

instance *id* **cost** *cost*

Syntax Description

id	MSTI ID. Range is 0 to 4094.
cost	Port cost. Range is 1 to 200000000.

Command Default

The default path cost depends on the speed of the link.

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the port cost to 10000 for the instance ID 101:

```
RP/0/RSP0/CPU0:router(config-mstp-if)# instance 101 cost 10000
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

instance port-priority

To set the port priority performance parameter for the MSTI, use the **instance port-priority** command in MSTP interface configuration submode.

instance *id* **port-priority** *priority*

Syntax Description

id	MSTI ID. Range is 0 to 4094.
priority	Port priority. Range is 0 to 240 in multiples of 16.

Command Default

priority: 128

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

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 set the port priority to 160 for the instance ID 101:

```
RP/0/RSP0/CPU0:router(config-mstp-if)# instance 101 port-priority 160
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

interface (MSTAG/REPAG)

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

interface {**Bundle-Ether| GigabitEthernet| TenGigE**} *instance.subinterface*

Syntax Description

instance.subinterface	Physical interface instance, followed by the subinterface identifier. Naming notation is instance.subinterface, and a period between arguments is required as part of the notation. • Replace the instance argument with the following physical interface instance. Naming notation is rack/slot/module/port and a slash between values is required as part of the notation. ◦ rack—Chassis number of the rack. ◦ slot—Physical slot number of the card. ◦ module—Module number. A physical layer interface module (PLIM) is always 0. ◦ port—Physical port number of the interface. • Replace the subinterface argument with the subinterface value. Range is from 0 through 4095.

Command Default

None

Command Modes

MSTAG configuration, REPAG configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

The specified subinterface must be configured to match untagged packets, i.e., it must be configured with **encapsulation untagged**. Only a single subinterface on any given port may be specified.

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 MSTAG interface configuration submode:

```
RP/0/RSP0/CPU0:router(config-mstag)# interface GigabitEthernet0/2/0/30.1
RP/0/RSP0/CPU0:router(config-mstag-if)#
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

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 {**Bundle-Ether| GigabitEthernet| TenGigE**} *instance*

Syntax Description

instance	Forward interface in rack/slot/instance/port format.

Command Default

None

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

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:

```
RP/0/RSP0/CPU0:router(config-mstp)# interface GigabitEthernet 0/0/0/1
RP/0/RSP0/CPU0:router(config-mstp-if)#
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

interface (PVSTAG/PVRSTAG)

To enter PVST or PVRST Access Gateway Interface configuration submode and to enable either PVSTAG or PVRSTAG for the specified port, use the **interface** command in PVST and PVRST Access Gateway configuration submode.

interface {**GigabitEthernet| TenGigE**} *instance*

Syntax Description

instance	Forward interface in rack/slot/instance/port format.

Command Default

None

Command Modes

PVSTAG and PVRSTAG configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter the PVST or PVRST Access Gateway Interface configuration submode:

```
RP/0/RSP0/CPU0:router(config-pvstag)# interface GigabitEthernet 0/0/0/1
RP/0/RSP0/CPU0:router(config-pvstag-if)#
```

Related Commands

Command	Description
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.

Command	Description
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

join-time

To set the join time for all active ports, use the **join-time** command in the MVRP configuration mode. To return to the default value, use the **no** form of this command.

join-time *interval*

no join-time *interval*

Syntax Description

interval	Maximum time for the join timer parameter for all active ports. The range is from 100 to 1000. The default value is 200.

Command Default

The default is 200 milliseconds.

Command Modes

MVRP configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the join time for active ports:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# spanning-tree mst AA
RP/0/RSP0/CPU0:router(config-mstp)# mvrp static
RP/0/RSP0/CPU0:router(config-mvrp)# periodic transmit interval 5
RP/0/RSP0/CPU0:router(config-mvrp)# join-time 200
!
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.

leave-time

To set the leave time for all active ports, use the **leave-time** command in the MVRP configuration mode. To return to the default value, use the **no** form of this command.

leave-time *interval*

no leave-time *interval*

Syntax Description

interval	Minimum time, in seconds, for the leaveall timer parameter for all active ports. The range is from 1 to 90 seconds .

Command Default

The default is 30 seconds.

Command Modes

MVRP configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the join time for active ports:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# spanning-tree mst AA
RP/0/RSP0/CPU0:router(config-mstp)# mvrp static
RP/0/RSP0/CPU0:router(config-mvrp)# periodic transmit interval 5
RP/0/RSP0/CPU0:router(config-mvrp)# leave-time 30!
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.

Command	Description
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.

leaveall-time

To set the leave all time for all active ports, use the **leaveall-time** command in the MVRP configuration mode. To return to the default value, use the **no** form of this command.

leaveall-time *interval*

no leaveall-time *interval*

Syntax Description

interval	Minimum time, in seconds, for the leaveall timer parameter for all active ports. The range is from 5 to 30 seconds.

Command Default

The default is 10 seconds.

Command Modes

MVRP configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the join time for active ports:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# spanning-tree mst AA
RP/0/RSP0/CPU0:router(config-mstp)# mvrp static
RP/0/RSP0/CPU0:router(config-mvrp)# periodic transmit interval 5
RP/0/RSP0/CPU0:router(config-mvrp)# leaveall-time 20
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.

Command	Description
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.

link-type

To set the link type of the port to point-to-point or multipoint, use the **link-type** command in MSTP interface configuration submode.

link-type {**point-to-point**| **multipoint**}

Syntax Description

This command has no keywords or arguments.

Command Default

The default value is derived from the duplex setting for the link. A full-duplex link is considered point-to-point, and all others are considered multipoint.

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the link type of the port to point-to-point:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# spanning-tree mst A
RP/0/RSP0/CPU0:router(config-mstp)# interface GigabitEthernet 0/3/0/3
RP/0/RSP0/CPU0:router(config-mstp-if)# link-type point-to-point
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.

Command	Description
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

max age

To set the maximum age for BPDUs sent on this interface, use the **max age** command in MSTAG interface configuration, REPAG interface configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

max age *seconds*

Syntax Description

seconds	Maximum age time for the bridge in seconds. Range is 6 to 40.

Command Default

seconds: 20

Command Modes

MSTAG interface configuration, REPAG interface configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG VLAN and PVRSTAG VLAN configuration modes.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services (PVSTAG and PVRSTAG only)	read, write
interface (MSTAG and REPAG only)	read, write

Examples

The following example shows how to set the maximum age time for the bridge to 20:

```
RP/0/RSP0/CPU0:router(config-mstag-if)# max age 20
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

maximum age

To set the maximum age parameter for the bridge, use the **maximum age** command in MSTP configuration submode.

maximum age *seconds*

Syntax Description

seconds	Maximum age time for the bridge in seconds. Range is 6 to 40.

Command Default

seconds: 20

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the maximum age time for the bridge to 40:

```
RP/0/RSP0/CPU0:router(config-mstp)# maximum age 40
```

Related Commands

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode

maximum hops (MSTP)

To set the maximum hops parameters for the bridge, use the **maximum hops** command in MSTP configuration submode.

maximum hops *hops*

Syntax Description

hops	Maximum number of hops for the bridge in seconds. Range is 6 to 40.

Command Default

hops: 20

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the maximum number of hops for the bridge to 30:

```
RP/0/RSP0/CPU0:router(config-mstp)# max hops 30
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

Command	Description
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

mvrp static

To enable Multiple VLAN Registration Protocol (MVRP) in static mode and to enter the MVRP configuration submode, use the **mvrp static** command in the MSTP configuration mode. To return to the default setting, use the **no** form of this command.

mvrp static

no mvrp static

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable MVRP static mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# spanning-tree mst AA
RP/0/RSP0/CPU0:router(config-mstp)# mvrp static
RP/0/RSP0/CPU0:router(config-mvrp)#
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.

Command	Description
join-time, on page 358	Sets the join time for all active ports.
leave-time, on page 360	Sets the leave time for all active ports.
leaveall-time, on page 362	Sets the leave all time for all active ports.
periodic transmit, on page 377	Sends periodic Multiple VLAN Registration Protocol Data Unit (MVRPDU) on all active ports.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

name (MSTAG/REPAG)

To set the name of the MSTP region, use the **name** command in MSTAG interface configuration or REPAG interface configuration submode.

name *name*

Syntax Description

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

Command Default

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

Command Modes

MSTAG interface configuration, REPAG interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RSP0/CPU0:router(config-mstag-if)# name leo
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.

Command	Description
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

name (MSTP)

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

name *name*

Syntax Description

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

Command Default

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

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RSP0/CPU0:router(config-mstp)# name m1
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

periodic transmit

To send periodic Multiple VLAN Registration Protocol Data Unit (MVRPDU) on all active ports, use the **periodic transmit** command in the MVRP configuration mode. To return to the default value, use the **no** form of this command.

periodic transmit [**interval** *interval*]

no periodic transmit [**interval** *interval*]

Syntax Description

interval *interval*	Sends periodic MVRPDU on all active ports at specified time interval. The range is from 2 to 10 seconds.

Command Default

The default is 3 seconds.

Command Modes

MVRP configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Sending periodic messages is not required when the state machines operate correctly. The periodic messages are intended purely to cope with a succession of lost new declaration MVRPDUs. In the absence of periodic messages, declarations are re-sent every 10 to 15 seconds in response to the LeaveAll timer expiring.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable MVRP static mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# spanning-tree mst AA
RP/0/RSP0/CPU0:router(config-mstp)# mvrp static
RP/0/RSP0/CPU0:router(config-mvrp)# periodic transmit interval 5
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.

port-id

To set the port ID for the current switch, use the **port-id** command in MSTAG interface configuration, REPAG interface configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

port-id *id* [**startup-value** *startup-id*]

Syntax Description

id	Interface port ID. For MSTAG, REPAG and PVRSTAG the allowed range is between 1 to 4095. For PVSTAG the allowed range is between 1 to 255.
startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-id	Sets the startup port ID.

Command Default

If a startup value is not specified, it defaults to the normal value.

Command Modes

MSTAG interface configuration, REPAG interface configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG VLAN and PVRSTAG VLAN configuration modes.

Usage Guidelines

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

This command is used when configuring Access Gateway, to set the value of the port ID advertised in BPDUs sent on this interface.

Task ID

Task ID	Operations
ethernet-services (PVSTAG and PVRSTAG only)	read, write
interface (MSTAG and REPAG only)	read, write

Examples

The following example shows how to set the port ID:

```
RP/0/RSP0/CPU0:router(config-mstag-if)# port-id 111
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
instance (MSTAG/REPAG), on page 344	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

port-priority

To set the port priority performance parameter for the MSTI, use the **port-priority** command in MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

port-priority *priority* [**startup-value** *startup-priority*]

Syntax Description

priority	Port priority. For MSTAG, REPAG and PVRSTAG, the range is between 0 to 40 in multiples of 16. For PVSTAG, the range is between 0 to 255.
startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-priority	Sets the startup port priority.

Command Default

If no startup-value is configured, the normal value is used during startup.

Command Modes

MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG VLAN and PVRSTAG VLAN configuration modes.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services (PVSTAG and PVRSTAG only)	read, write
interface (MSTAG and REPAG only)	read, write

Examples

The following example shows how to set the port priority to 160:

```
RP/0/RSP0/CPU0:router(config-mstag-if-inst)# port-priority 160
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
instance (MSTAG/REPAG), on page 344	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

portfast

To enable PortFast 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 3.7.1	This command was introduced.

Usage Guidelines

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

This command enables the portfast feature (also known as edge port). When this is enabled, MSTP treats the port as an edge port, i.e., it keeps it in forwarding state and does not generate topology changes if the port goes down or comes up. It is not expected to receive MSTP BPDUs on an edge port. BPDU guard is a Cisco extension that causes the interface to be shut down using error-disable if an MSTP BPDU is received. For more information on portfast feature, refer to the *Implementing Multiple Spanning Tree Protocol* module in the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RSP0/CPU0:router(config-mstp-if)# portfast
RP/0/RSP0/CPU0:router(config-mstp-if)# portfast bpduguard
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

preempt delay

To enable topology control and set the preempt delay on startup, use the **preempt delay** command in MSTAG, REPAG, PVSTAG or PVRSTAG configuration mode.

preempt delay {**for** *time* {**seconds**| **minutes**| **hours**}| **until** *hh*:*mm*:*ss*}

Syntax Description

for	Specifies length of time to delay preempting for in seconds, minutes or hours.
until	Specifies time to delay preempting until the mentioned interval (24-hour hh:mm:ss).

Command Default

Startup topology control is disabled.

Command Modes

MSTAG configuration, REPAG configuration, PVSTAG configuration, PVRSTAG configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG and PVRSTAG configuration modes.

Usage Guidelines

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

This command enables startup topology control for Access Gateway. By default, when an interface comes up, Access Gateway starts sending STP BPDUs immediately based on the configured values. This could cause the devices in the access network to immediately start directing traffic to this device. However, the data plane may not yet be ready to forward packets to the core or aggregation network. When a preempt delay is configured, alternative values are sent in the BPDUs for the specified time. These alternative values must be configured using the **startup-value** option, and can be set so as to cause the access devices not to use this link unless it is the only one available.

For more information on preempt delay, refer to the *Implementing Multiple Spanning Tree Protocol* module in the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*.

Task ID

Task ID	Operations
ethernet-services (PVSTAG and PVRSTAG only)	read, write

Task ID	Operations
interface (MSTAG and REPAG only)	read, write

Examples

The following example shows how to set the preempt delay for 20 seconds:

```
RP/0/RSP0/CPU0:router(config-mstag)# preempt delay for 20 seconds
```

Related Commands

Command	Description
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

priority (Access Gateway)

To set the bridge priority for the current MSTI or VLAN, use the **priority** command in the MSTAG, REPAG, PVSTAG or PVRSTAG instance configuration submodes.

priority *priority* [**startup-value** *startup-priority*]

Syntax Description

priority	Specifies the bridge priority. For MSTAG, REPAG and PVRSTAG, the range is between 0 to 61440 in multiples of 4096. For PVSTAG, the range is between 0 to 65535.
startup-value	Sets an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-priority	Specifies the startup priority.

Command Default

Default value is 32768. If the startup value is not specified while the standard value is, the startup value defaults to the standard value.

Command Modes

MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG and PVRSTAG configuration mode.

Usage Guidelines

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

This command is used when configuring Access Gateway to set the bridge priority that is advertised for this MSTI or VLAN in the BPDUs sent from this interface.

Task ID

Task ID	Operations
ethernet-services (PVSTAG and PVRSTAG only)	read, write
interface (MSTAG and REPAG only)	read, write

Examples

The following example shows how to set the bridge priority for the current MSTI:

```
RP/0/RSP0/CPU0:router(config-mstag-if-inst)# priority 4096 startup-value 32768
```

Related Commands

Command	Description
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.

priority (MSTP)

To set the bridge priority for the current MSTI, use the **priority** command in MSTI configuration submode.

priority *priority*

Syntax Description

priority	Bridge priority for the current MSTI. Range is 0 to 61440 in multiples of 4096.

Command Default

priority: 32768

Command Modes

MSTI configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the bridge priority to 8192 for the current MSTI:

```
RP/0/RSP0/CPU0:router(config-mstp-inst)# priority 8192
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
instance (MSTP), on page 346	Enters the multiple spanning tree instance (MSTI) configuration submode.

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

provider-bridge (MSTAG/REPAG)

To place the current instance of the protocol in 802.1ad mode, use the **provider-bridge** command in MSTAG or REPAG interface configuration submode.

provider-bridge

Syntax Description

This command has no keywords or arguments.

Command Default

The default value is FALSE.

Command Modes

MSTAG interface configuration, REPAG interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to use the **provider-bridge** command:

```
RP/0/RSP0/CPU0:router(config-mstag-if)# provider-bridge
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.

Command	Description
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

provider-bridge (MSTP)

To place the current instance of the protocol in 802.1ad mode, use the **provider-bridge** command in MSTP configuration submode.

provider-bridge

Syntax Description

This command has no keywords or arguments.

Command Default

The default value is FALSE.

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to use the **provider-bridge** command:

```
RP/0/RSP0/CPU0:router(config-mstp)# provider-bridge
```

Related Commands

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode

revision (MSTAG/REPAG)

To set the revision level in the BPDUs sent from this interface, use the **revision** command in MSTAG or REPAG interface configuration submode.

revision *revision-number*

Syntax Description

revision-number	Revision level of the MSTP region. Range is 0 to 65535.

Command Default

revision-number: 0

Command Modes

MSTAG interface configuration, REPAG interface configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the revision level of the MSTP region to 1:

```
RP/0/RSP0/CPU0:router(config-mstag-if)# revision 1
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.

Command	Description
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

revision (MSTP)

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

revision *revision-number*

Syntax Description

revision-number	Revision level of the MSTP region. Range is 0 to 65535.

Command Default

revision-number: 0

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the revision level of the MSTP region to 10:

```
RP/0/RSP0/CPU0:router(config-mstp)# revision 10
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

Command	Description
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

root-cost

To set the root path cost to sent in BPDUs from this interface, use the **root-cost** command in PVSTAG VLAN configuration or PVRSTAG VLAN configuration mode.

root-cost *cost* [**startup-value** *startup-cost*]

Syntax Description

cost	Sets the root path cost for the current port. The cost ranges between 0 to 4294967295.
startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-cost	Sets the startup cost.

Command Default

The default is 0. If a cost is configured but no startup value is configured, the startup value defaults to the configured cost value. If no cost is configured, the startup value defaults to 1.

Command Modes

PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to set the root path cost for the current port:

```
RP/0/RSP0/CPU0:router(config-pvrstag-if-vlan)# root-cost 1000000
```

Related Commands

Command	Description
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

root-id

To set the identifier of the root bridge for BPDUs sent from a port and an optional startup-value, use the **root-id** command in the MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration and PVRSTAG VLAN configuration modes.

root-id *id* [**startup-value** *startup-id*]

Syntax Description

id	Sets the root bridge ID (MAC address) to set in the BPDUs.
startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-id	Sets the startup root ID.

Command Default

The MAC address of the region root switch. If the startup value is not specified while the standard value is, the startup value defaults to the standard value. For MSTAG and REPAG, the default is the bridge ID. For PVSTAG and PVRSTAG, the default is 0000.0000.0000.

Command Modes

MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG VLAN and PVRSTAG VLAN configuration modes.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services (PVSTAG and PVRSTAG only)	read, write
interface (MSTAG and REPAG only)	read, write

Examples

The following example shows how to set the identifier of the root bridge for BPDUs:

```
RP/0/RSP0/CPU0:router(config-pvstag-if-vlan)#root-id 0000.0000.0000 startup-value
0000.0000.0001
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
instance (MSTAG/REPAG), on page 344	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

root-priority

To set the root bridge priority sent in BPDUs for this interface for this MSTI or VLAN, and to set an optional startup value, use the **root-priority** command in the MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration and PVRSTAG VLAN configuration modes.

root-priority *priority* [**startup-value** *startup-priority*]

Syntax Description

priority	Sets the root bridge priority to set in the BPDUs. For MSTAG, REPAG and PVRSTAG, the range is between 0 to 61440 in multiples of 4096. For PVSTAG, the range is between 0 to 65535.
startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
startup-priority	Sets the startup root priority.

Command Default

Default value is 32768. If the startup value is not specified while the standard value is, the startup value defaults to the standard value.

For MSTAG and REPAG, the default is 32768. For PVSTAG and PVRSTAG, the default is 0.

Command Modes

MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG VLAN and PVRSTAG VLAN configuration modes.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services (PVSTAG and PVRSTAG only)	read, write
interface (MSTAG and REPAG only)	read, write

Examples

The following example shows how to set the root bridge priority for the current MSTI:

```
RP/0/RSP0/CPU0:router(config-pvstag-if-vlan)# root-priority 4096 startup-value 8192
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
instance (MSTAG/REPAG), on page 344	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

show ethernet mvrp mad

To display the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port, for each active attribute value (VID), use the **show ethernet mvrp mad** command in EXEC mode.

show ethernet mvrp mad [brief] [**interface** *interface-name*] [**vlan** *vlan-id*]

Syntax Description

brief	(Optional) Displays a brief view.
interface	(Optional) Displays the MVRP state for the given subinterface or base interface name.
interface-name	(Optional) Displays the interface name.
vlan *vlan-id*	(Optional) Displays information for a particular VLAN. The range is between 0 to 4094.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following sample output is from the **show ethernet mvrp mad** command:

```
RP/0/RSP0/CPU0:router# show ethernet mvrp mad interface GigabitEthernet 0/1/0/1
GigabitEthernet0/1/0/1
  Participant Type: Full; Point-to-Point: Yes
  Admin Control: Applicant Normal; Registrar Normal

  LeaveAll Passive (next in 5.92s); periodic disabled
  Leave in 25.70s; Join not running
  Last peer 0293.6926.9585; failed registrations: 0

VID   Applicant             Registrar
----  ---------------------  ---------
   1  Very Anxious Observer  Leaving
 283  Quiet Passive          Empty
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.

show ethernet mvrp statistics

To display packet statistics per port, use the **show ethernet mvrp statistics** command in EXEC mode.

show ethernet mvrp statistics [**interface** *type interface-path-id*]

Syntax Description

interface	(Optional) Displays the MVRP state for the given subinterface or base interface name.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following sample output is from the **show ethernet mvrp statistics** command:

```
RP/0/RSP0/CPU0:router# show ethernet mvrp statistics interface GigabitEthernet 0/1/0/1
GigabitEthernet0/1/0/1
```

```
MVRPDUs TX:    1245
MVRPDUs RX:       7
Dropped TX:       0
Dropped RX:      42
Invalid RX:      12
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp status, on page 408	Displays a summary of the VIDs that are declared or registered.

show ethernet mvrp status

To display a summary of the VIDs that are declared or registered, and to learn the origin of these declarations, use the **show ethernet mvrp status** command in EXEC mode.

show ethernet mvrp status [**interface** *type interface-path-id*]

Syntax Description

interface	(Optional) Displays the MVRP state for the given subinterface or base interface name.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following sample output is from the **show ethernet mvrp status** command:

```
RP/0/RSP0/CPU0:router# show ethernet mvrp status interface GigabitEthernet 0/1/0/1
```

```
GigabitEthernet0/1/0/1
  Statically declared:  1-512,768,980-1034
  Dynamically declared: 2048-3084
  Registered:           1-512
```

Related Commands

Command	Description
debug ethernet mvrp packets, on page 308	Enables debugging of sent and received MVRP packets.
debug ethernet mvrp protocol, on page 310	Enables MVRP protocol debugging on a specific interface, location or vlan.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show ethernet mvrp mad, on page 404	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 406	Displays packet statistics per port.

show l2vpn mstp port

To display the internal MSTI number and number of ports for each VLAN, use the **show l2vpn mstp port** command in EXEC mode.

show l2vpn mstp port [**interface** *type interface-path-id*] [**msti** *value*]

Syntax Description

interface	(Optional) Displays the MSTP state for the given interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.
msti *value*	(Optional) Displays the filter for Multiple Spanning Tree Instance (MSTI). The range is from 0 to 100.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn mstp port interface gigabitethernet 0/1/0/0 msti 5
```

Related Commands

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
show l2vpn mstp vlan, on page 412	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.

show l2vpn mstp vlan

To display the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface, use the **show l2vpn mstp vlan** command in EXEC mode.

show l2vpn mstp vlan [**interface** *type interface-path-id*] [**msti** *value*] [**vlan-id** *value*]

Syntax Description

interface	(Optional) Displays the MSTP state for the given subinterface or base interface name.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **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.
msti *value*	(Optional) Displays the filter for Multiple Spanning Tree Instance (MSTI). The range is from 0 to 100.
vlan-id *value*	(Optional) Displays the filter for the VLAN ID. The range is from 0 to 4294967295.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn mstp vlan interface gigabitethernet 0/1/0/0 msti 5 vlan-id
 5
```

Related Commands

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree mst, on page 445	Enters the MSTP configuration submode
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
show l2vpn mstp port, on page 410	Displays the internal MSTI number and number of ports for each VLAN.

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 3.7.1	This command was introduced.
Release 3.9.1	The **topology-change** keyword was added.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

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

```
RP/0/RSP0/CPU0:router# show spanning-tree mst a instance 0
```

```
Operating in Provider Bridge mode
MSTI 0 (CIST):

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

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


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

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

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

```
RP/0/RSP0/CPU0:router# show spanning-tree mst a brief
MSTI 0 (CIST):
  VLAN IDs: 1-100, 500-1000, 1017
  This is the Root Bridge
MSTI 1:
  VLAN IDS: 101-499
  Root Port GigabitEthernet0/1/2/2  , Root Bridge ID 0002.9b78.0812
...
RP/0/RSP0/CPU0:router# show spanning-tree mst blocked-ports
MSTI 0 (CIST):

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

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
show l2vpn mstp port, on page 410	Displays the internal MSTI number and number of ports for each VLAN.
show l2vpn mstp vlan, on page 412	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
show spanning-tree mst bpdu interface, on page 417	Displays the contents of MSTP BPDUs being sent and received on a particular interface.
show spanning-tree mst configuration, on page 419	Displays the VLAN ID to MSTI mapping table.
show spanning-tree mst errors, on page 421	Displays information about misconfiguration affecting MSTP.

Command	Description
show spanning-tree mst interface, on page 423	Displays detailed information on the interface state.
show spanning-tree mst topology-change flushes, on page 426	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

show spanning-tree mst bpdu interface

To display the contents of MSTP BPDUs being sent and received on a particular interface, use the **show spanning-tree mst bpdu interface** command in the EXEC mode.

show spanning-tree mst *protocol instance identifier* **bpdu interface** *type interface-path-id* [**direction** {**receive**| **transmit**}]

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
bpdu interface	Displays multiple spanning tree BPDUs.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.
direction	Displays per-interface MST BPDUs for a specific direction.
receive	Displays only the MST BPDUs received on this interface.
transmit	Displays only the MST BPDUs being transmitted for this interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mst** command, which produces details on the BPDUs being output and received on a given local interface:

Note Several received packets can be stored in case of MSTP operating on a shared LAN.

```
RP/0/RSP0/CPU0:router# show spanning-tree mst a bpdu interface GigabitEthernet0/1/2/2
direction transmit
MSTI 0 (CIST):
Root ID : 0004.9b78.0800
Path Cost : 83
Bridge ID : 0004.9b78.0800
Port ID : 12
Hello Time : 2
...
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
show l2vpn mstp port, on page 410	Displays the internal MSTI number and number of ports for each VLAN.
show l2vpn mstp vlan, on page 412	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.
show spanning-tree mst configuration, on page 419	Displays the VLAN ID to MSTI mapping table.
show spanning-tree mst errors, on page 421	Displays information about misconfiguration affecting MSTP.
show spanning-tree mst interface, on page 423	Displays detailed information on the interface state.
show spanning-tree mst topology-change flushes, on page 426	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

show spanning-tree mst configuration

To display the VLAN ID to MSTI mapping table, use the **show spanning-tree mst configuration** command in the EXEC mode.

show spanning-tree mst *protocol instance identifier* **configuration**

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
configuration	Displays a summary of MST related configuration.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mst** command, which displays the VLAN ID to MSTI mapping table:

```
RP/0/RSP0/CPU0:router# show spanning-tree mst a configuration
Name          leo
Revision      2702
Config Digest 9D-14-5C-26-7D-BE-9F-B5-D8-93-44-1B-E3-BA-08-CE
Instance  Vlans mapped
--------  -------------------------------
0         1-9,11-19,21-29,31-39,41-4094
1         10,20,30,40
------------------------------------------
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
show l2vpn mstp port, on page 410	Displays the internal MSTI number and number of ports for each VLAN.
show l2vpn mstp vlan, on page 412	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.
show spanning-tree mst bpdu interface, on page 417	Displays the contents of MSTP BPDUs being sent and received on a particular interface.
show spanning-tree mst errors, on page 421	Displays information about misconfiguration affecting MSTP.
show spanning-tree mst interface, on page 423	Displays detailed information on the interface state.
show spanning-tree mst topology-change flushes, on page 426	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

show spanning-tree mst errors

To display information about misconfiguration affecting MSTP, use the **show spanning-tree mst errors** in the EXEC mode.

show spanning-tree mst *protocol instance identifier* **errors**

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
errors	Displays configuration errors for MST.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mst** command, which produces information about interfaces that are configured for MSTP but where MSTP is not operational. Primarily this shows information about interfaces which do not exist:

```
RP/0/RSP0/CPU0:router# show spanning-tree mst a errors
Interface                Error
------------------------------
GigabitEthernet1/2/3/4   Interface does not exist.
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
show l2vpn mstp port, on page 410	Displays the internal MSTI number and number of ports for each VLAN.
show l2vpn mstp vlan, on page 412	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.
show spanning-tree mst bpdu interface, on page 417	Displays the contents of MSTP BPDUs being sent and received on a particular interface.
show spanning-tree mst configuration, on page 419	Displays the VLAN ID to MSTI mapping table.
show spanning-tree mst interface, on page 423	Displays detailed information on the interface state.
show spanning-tree mst topology-change flushes, on page 426	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

show spanning-tree mst interface

To display detailed information on the interface state, use the **show spanning-tree mst interface** command in EXEC mode.

show spanning-tree mst *protocol instance identifier* **interface** *type interface-path-id* [**instance id**]

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
interface *type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.
instance *id*	Forward interface in rack/slot/instance/port format.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mst** command, which produces more detailed information regarding interface state than the standard command as described above:

```
RP/0/RSP0/CPU0:router# show spanning-tree mst a interface GigabitEthernet0/1/2/1 instance
3
GigabitEthernet0/1/2/1
Cost: 20000
link-type: point-to-point
hello-time 1
Portfast: no
BPDU Guard: no
Guard root: no
Guard topology change: no
BPDUs sent 492, received 3

MST 3:
Edge port:
Boundary : internal
Designated forwarding
Vlans mapped to MST 3: 1-2,4-2999,4000-4094
Port info port id 128.193 cost 200000
Designated root address 0050.3e66.d000 priority 8193 cost 20004
Designated bridge address 0002.172c.f400 priority 49152 port id 128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Transitions to reach this state: 12
```

The output includes interface information about the interface which applies to all MSTIs:

- Cost
- link-type
- hello-time
- portfast (including whether BPDU guard is enabled)
- guard root
- guard topology change
- BPDUs sent, received.

It also includes information specific to each MSTI:

- Port ID, priority, cost
- BPDU information from root (bridge ID, cost, and priority)
- BPDU information being sent on this port (Bridge ID, cost, priority)
- State transitions to reach this state.
- Topology changes to reach this state.

```
Flush containment status for this MSTI.
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.

Command	Description
show l2vpn mstp port, on page 410	Displays the internal MSTI number and number of ports for each VLAN.
show l2vpn mstp vlan, on page 412	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.
show spanning-tree mst bpdu interface, on page 417	Displays the contents of MSTP BPDUs being sent and received on a particular interface.
show spanning-tree mst configuration, on page 419	Displays the VLAN ID to MSTI mapping table.
show spanning-tree mst errors, on page 421	Displays information about misconfiguration affecting MSTP.
show spanning-tree mst topology-change flushes, on page 426	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

show spanning-tree mst topology-change flushes

To display details of the last topology change that occurred for each pair of port and instance, as well as a count of the number of topology changes at each port, use the **show spanning-tree mst topology-change flushes** command in the EXEC mode.

show spanning-tree mst protocol instance identifier topology-change flushes [**instance** *id*] [**interface** *type interface-path-id*| **latest**]

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
topology-change	Displays topology change information.
flushes	Displays latest topology change flushes for each interface.
instance *id*	Instance for which information needs to be displayed.
interface *type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.
latest	Displays the most recent topology change for each instance.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Note The latest filter displays only the most recent topology change for each instance. The output also displays information of the flush operation that takes place when the flush containment is active on an MSTI for a port.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mst** command, which displays details on the MSTIs :

```
RP/0/RSP0/CPU0:router# show spanning-tree mst M topology-change flushes instance$
MSTI 1:

Interface     Last TC               Reason                            Count
------------  --------------------  --------------------------------  -----
Te0/0/0/1     04:16:05 Mar 16 2010  Role change: DSGN to ----            10
#
#
RP/0/RSP0/CPU0:router# show spanning-tree mst M topology-change flushes instance$
MSTI 0 (CIST):

Interface     Last TC               Reason                            Count
------------  --------------------  --------------------------------  -----
Te0/0/0/1     04:16:05 Mar 16 2010  Role change: DSGN to ----            10
#
#
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
show l2vpn mstp port, on page 410	Displays the internal MSTI number and number of ports for each VLAN.
show l2vpn mstp vlan, on page 412	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.
show spanning-tree mst bpdu interface, on page 417	Displays the contents of MSTP BPDUs being sent and received on a particular interface.
show spanning-tree mst configuration, on page 419	Displays the VLAN ID to MSTI mapping table.

Command	Description
show spanning-tree mst errors, on page 421	Displays information about misconfiguration affecting MSTP.
show spanning-tree mst interface, on page 423	Displays detailed information on the interface state.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

show spanning-tree mstag

To display the values currently used for populating the BPDUs sent by all ports (with the specified feature enabled), use the **show spanning-tree mstag** in the EXEC mode.

show spanning-tree mstag *protocol instance identifier*

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.
Release 4.1.0	The show output of this command was modified to include information on the MSTAG Edge Mode feature.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

This example shows the output from the **show spanning-tree mstag** command:

```
RP/0/RSP0/CPU0:router# show spanning-tree mstag A
GigabitEthernet0/0/0/1
  Preempt delay is disabled.
  Name:            6161:6161:6161
  Revision:        0
  Max Age:         20
  Provider Bridge: no
  Bridge ID:       6161.6161.6161
  Port ID:         1
  External Cost:   0
```

```
    Hello Time:      2
    Active:          no
    BPDUs sent:      0
      MSTI 0 (CIST):
      VLAN IDs:         1-9,32-39,41-4094
      Role:             Designated
      Bridge Priority:  32768
      Port Priority:    128
      Cost:             0
      Root Bridge:      6161.6161.6161
      Root Priority:    32768
      Topology Changes: 123
    MSTI 2
      VLAN IDs:         10-31
      Role:             Designated
      Bridge Priority:  32768
      Port Priority:    128
      Cost:             0
      Root Bridge:      6161.6161.6161
      Root Priority:    32768
      Topology Changes: 123
    MSTI 10
   VLAN IDs:         40
      Role:             Root (Edge mode)
      Bridge Priority:  32768
      Port Priority:    128
      Cost:             200000000
      Root Bridge:      6161.6161.6161
      Root Priority:    61440
      Topology Changes: 0
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
show spanning-tree mstag bpdu interface, on page 431	Displays the content of the BPDUs being sent from this interface.
show spanning-tree mstag topology-change flushes, on page 433	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.

show spanning-tree mstag bpdu interface

To view the content of the BPDUs being sent from this interface, use the **show spanning-tree mstag bpdu interface** command in the EXEC mode.

show spanning-tree mstag *protocol instance identifier* **bpdu interface** *type interface-path-id*

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
bpdu interface	Displays multiple spanning tree BPDUs.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mstag bpdu interface** command:

```
RP/0/RSP0/CPU0:router#show spanning-tree mstag foo bpdu interface GigabitEthernet 0/0/0/0
Transmitted:
  MSTI 0 (CIST):
ProtocolIdentifier: 0
ProtocolVersionIdentifier: 3
BPDUType: 2
CISTFlags: Top Change Ack  0
           Agreement       1
           Forwarding      1
           Learning        1
           Role            3
           Proposal        0
           Topology Change 0
CISTRootIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTExternalPathCost: 0
CISTRegionalRootIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTPortIdentifierPriority: 8
CISTPortIdentifierId: 1
MessageAge: 0
MaxAge: 20
HelloTime: 2
ForwardDelay: 15
Version1Length: 0
Version3Length: 80
FormatSelector: 0
Name: 6969:6969:6969
Revision: 0
MD5Digest: ac36177f 50283cd4 b83821d8 ab26de62
CISTInternalRootPathCost: 0
CISTBridgeIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTRemainingHops: 20
  MSTI 1:
MSTIFlags: Master          0
           Agreement       1
           Forwarding      1
           Learning        1
           Role            3
           Proposal        0
           Topology Change 0
MSTIRegionalRootIdentifier: priority 8, MSTI 1, address 6969.6969.6969
MSTIInternalRootPathCost: 0
MSTIBridgePriority: 1
MSTIPortPriority: 8
MSTIRemainingHops: 20
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree mstag topology-change flushes, on page 433	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.

show spanning-tree mstag topology-change flushes

To display details of the last topology change that occurred for each pair of port and instance, as well as a count of the number of topology changes at each port, use the **show spanning-tree mstag topology-change flushes** command in the EXEC mode.

Note The latest filter displays only the most recent topology change for each instance. The output also displays information of the flush operation that takes place when the flush containment is active on an MSTI for a port.

show spanning-tree mstag *protocol instance identifier* **topology-change flushes** [**instance** *id*] [**interface** *type interface-path-id*| **latest**]

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
topology-change	Displays topology change information.
flushes	Displays latest topology change flushes for each interface.
instance*id*	Forward interface in rack/slot/instance/port format.
interface *type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.
latest	Displays the most recent topology change for each instance.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mstag topology-change flushes** command, which displays details on the MSTIs :

```
RP/0/RSP0/CPU0:router# show spanning-tree mstag b topology-change flushes

MSTAG Protocol Instance b

Interface     Last TC              Reason                            Count
------------  -------------------  --------------------------------  -----
Gi0/0/0/1     18:03:24 2009-07-14  Gi0/0/0/1.10 egress TCN           65535
Gi0/0/0/2     21:05:04 2009-07-15  Gi0/0/0/2.1234567890 ingress TCN      2
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree mstag bpdu interface, on page 431	Displays the content of the BPDUs being sent from this interface.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.

show spanning-tree pvrstag

To display the values currently used for populating the BPDUs sent by all ports (with the specified feature enabled), use the **show spanning-tree pvrstag** in the EXEC mode.

show spanning-tree pvrstag *protocol instance identifier* [**interface** *type interface-path-id*]

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
interface *type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree pvrstag** command:

```
RP/0/RSP0/CPU0:router# show spanning-tree pvrstag interface GigabitEthernet0/0/0/1
GigabitEthernet0/0/0/1
```

```
VLAN 10
  Preempt delay is disabled.
  Sub-interface:    GigabitEthernet0/0/0/1.20 (Up)
  Max Age:          20
  Root Priority:    0
  Root Bridge:      0000.0000.0000
  Cost:             0
  Bridge Priority:  32768
  Bridge ID:        6161.6161.6161
  Port Priority:    128
  Port ID:          1
  Hello Time:       2
  Active:           no
  BPDUs sent:       0
  Topology Changes: 123
 VLAN 20
```

Related Commands

Command	Description
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.

show spanning-tree pvstag

To display the values currently used for populating the BPDUs sent by all ports (with the specified feature enabled), use the **show spanning-tree pvstag** in the EXEC mode.

show spanning-tree pvstag *protocol instance identifier* [**interface** *type interface-path-id*]

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
interface *type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree pvstag** command:

```
RP/0/RSP0/CPU0:router# show spanning-tree pvstag interface GigabitEthernet0/0/0/1
GigabitEthernet0/0/0/1
```

```
VLAN 10
  Preempt delay is disabled.
  Sub-interface:    GigabitEthernet0/0/0/1.20 (Up)
  Max Age:          20
  Root Priority:    0
  Root Bridge:      0000.0000.0000
  Cost:             0
  Bridge Priority:  32768
  Bridge ID:        6161.6161.6161
  Port Priority:    128
  Port ID:          1
  Hello Time:       2
  Active:           no
  BPDUs sent:       0
  Topology Changes: 123
 VLAN 20
```

show spanning-tree repag

To display the values currently used for populating the BPDUs sent by all ports (with the specified feature enabled), use the **show spanning-tree repag** in the EXEC mode.

show spanning-tree repag *protocol instance identifier* [**interface** *type interface-path-id*] **[brief]**

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
interface *type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree repag** command:

```
RP/0/RSP0/CPU0:router# show spanning-tree repag interface GigabitEthernet0/0/0/1
GigabitEthernet0/0/0/1
```

```
 VLAN 10
   Preempt delay is disabled.
   Sub-interface:    GigabitEthernet0/0/0/1.20 (Up)
   Max Age:          20
   Root Priority:    0
   Root Bridge:      0000.0000.0000
   Cost:             0
   Bridge Priority:  32768
   Bridge ID:        6161.6161.6161
   Port Priority:    128
   Port ID:          1
   Hello Time:       2
   Active:           no
   BPDUs sent:       0
   Topology Changes: 123
  VLAN 20
```

Related Commands

Command	Description
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
show spanning-tree repag bpdu interface, on page 441	Displays BPDU information from root (bridge ID, cost, and priority) and the BPDU information being sent on the port.
show spanning-tree repag topology-change flushes, on page 443	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.

show spanning-tree repag bpdu interface

To display BPDU information from root (bridge ID, cost, and priority) and the BPDU information being sent on the port (Bridge ID, cost, priority) specific to an MSTI, use the show **spanning-tree repag bpdu interface** command in the EXEC mode.

show spanning-tree repag *protocol instance identifier* [**bpdu interface** *type interface-path-id*]

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
bpdu interface	Displays multiple spanning tree BPDUs.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree repag** command, which produces details on the BPDUs being output and received on a given local interface:

```
RP/0/RSP0/CPU0:router#show spanning-tree mstag foo bpdu interface GigabitEthernet 0/0/0/0
Transmitted:
  MSTI 0 (CIST):
ProtocolIdentifier: 0
ProtocolVersionIdentifier: 3
BPDUType: 2
CISTFlags: Top Change Ack  0
           Agreement       1
           Forwarding      1
           Learning        1
           Role            3
           Proposal        0
           Topology Change 0
CISTRootIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTExternalPathCost: 0
CISTRegionalRootIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTPortIdentifierPriority: 8
CISTPortIdentifierId: 1
MessageAge: 0
MaxAge: 20
HelloTime: 2
ForwardDelay: 15
Version1Length: 0
Version3Length: 80
FormatSelector: 0
Name: 6969:6969:6969
Revision: 0
MD5Digest: ac36177f 50283cd4 b83821d8 ab26de62
CISTInternalRootPathCost: 0
CISTBridgeIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTRemainingHops: 20
  MSTI 1:
MSTIFlags: Master          0
           Agreement       1
           Forwarding      1
           Learning        1
           Role            3
           Proposal        0
           Topology Change 0
MSTIRegionalRootIdentifier: priority 8, MSTI 1, address 6969.6969.6969
MSTIInternalRootPathCost: 0
MSTIBridgePriority: 1
MSTIPortPriority: 8
MSTIRemainingHops: 20
```

Related Commands

Command	Description
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag topology-change flushes, on page 443	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.

show spanning-tree repag topology-change flushes

To display details of the last topology change that occurred for each pair of port and instance, as well as a count of the number of topology changes at each port, use the **show spanning-tree repag topology-change flushes** command in the EXEC mode.

Note The latest filter displays only the most recent topology change for each instance. The output also displays information of the flush operation that takes place when the flush containment is active on an MSTI for a port.

show spanning-tree repag *protocol instance identifier* **topology-change flushes** [**instance** *id*] [**interface** *type interface-path-id*| **latest**]

Syntax Description

protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.
topology-change	Displays topology change information.
flushes	Displays latest topology change flushes for each interface.
instance*id*	Forward interface in rack/slot/instance/port format.
interface *type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **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.
latest	Displays the most recent topology change for each instance.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree repag topology-change flushes** command, which displays details on the MSTIs :

```
RP/0/RSP0/CPU0:router#show spanning-tree repag b topology-change flushes

MSTAG Protocol Instance b

Interface     Last TC              Reason                            Count
------------  -------------------  --------------------------------  -----
Gi0/0/0/1     18:03:24 2009-07-14  Gi0/0/0/1.10 egress TCN           65535
Gi0/0/0/2     21:05:04 2009-07-15  Gi0/0/0/2.1234567890 ingress TCN      2
```

Related Commands

Command	Description
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag bpdu interface, on page 441	Displays BPDU information from root (bridge ID, cost, and priority) and the BPDU information being sent on the port.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) 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 3.7.1	This command was introduced.

Usage Guidelines

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

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:

```
RP/0/RSP0/CPU0:router(config)# spanning-tree mst a
RP/0/RSP0/CPU0:router(config-mstp)#
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
instance (MSTP), on page 346	Enters the multiple spanning tree instance (MSTI) configuration submode.
interface (MSTP), on page 354	Enters the MSTP interface configuration submode, and enables STP for the specified port.
mvrp static, on page 371	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

spanning-tree mstag

To enter the MST Access Gateway configuration submode, use the **spanning-tree mstag** command in global configuration mode.

spanning-tree mstag *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 3.7.1	This command was introduced.

Usage Guidelines

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

Refer to the *Implementing Multiple Spanning Tree Protoco*l module of the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide* for more information.

Note Unlike MSTP configuration, multiple MSTAG instances can be configured concurrently.

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RSP0/CPU0:router(config)# spanning-tree mstag a
RP/0/RSP0/CPU0:router(config-mstag)#
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
instance (MSTAG/REPAG), on page 344	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.

spanning-tree pvrstag

To enter the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode, use the **spanning-tree pvrstag** command in global configuration mode.

spanning-tree pvrstag *protocol instance identifier*

Syntax Description

protocol instance identifier	String of a maximum of 255 characters that identifies the protocol instance.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Refer to the *Implementing Multiple Spanning Tree Protoco*l module of the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide* for more information.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

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

```
RP/0/RSP0/CPU0:router(config)# spanning-tree pvrstag a
RP/0/RSP0/CPU0:router(config-pvrstag)#
```

Related Commands

Command	Description
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.

Command	Description
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

spanning-tree pvstag

To enter the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode, use the **spanning-tree pvstag** command in global configuration mode.

spanning-tree pvstag *protocol instance identifier*

Syntax Description

protocol instance identifier	String of a maximum of 255 characters that identifies the protocol instance.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Refer to the *Implementing Multiple Spanning Tree Protoco*l module of the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide* for more information.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter the PVSTAG configuration mode:

```
RP/0/RSP0/CPU0:router(config)# spanning-tree pvstag a
RP/0/RSP0/CPU0:router(config-pvstag)#
```

Related Commands

Command	Description
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.

Command	Description
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 457	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

spanning-tree repag

To enter the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode, use the **spanning-tree repag** command in global configuration mode.

spanning-tree repag *protocol instance identifier*

Syntax Description

protocol instance identifier	String of a maximum of 255 characters that identifies the protocol instance.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Refer to the *Implementing Multiple Spanning Tree Protoco*l module of the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide* for more information.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the REPAG configuration mode:

```
RP/0/RSP0/CPU0:router(config)# spanning-tree repag a
RP/0/RSP0/CPU0:router(config-repag)#
```

Related Commands

Command	Description
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.

Command	Description
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
instance (MSTAG/REPAG), on page 344	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

transmit hold-count

To set the transmit hold count performance parameter, use the **transmit hold-count** command in MSTP configuration submode.

transmit hold-count *count*

Syntax Description

count	Bridge transmit hold count. Range is 1 to 10.

Command Default

count: 6

Command Modes

MSTP configuration

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the bridge transmit hold-count parameter to 8:

```
RP/0/RSP0/CPU0:router(config)# spanning-tree mst A
RP/0/RSP0/CPU0:router(config-mstp)# transmit hold-count 8
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
spanning-tree mst, on page 445	Enters the MSTP configuration submode

Command	Description
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

vlan

To enable a PVST or PVRST VLAN instance on the interface and enter PVSTAG or PVRSTAG VLAN configuration mode, use the **vlan** command in PVSTAG or PVRSTAG configuration submode.

vlan *vlan-id*

Syntax Description

vlan-id	Specifies the VLAN identifier. The range of the VLAN ID is between 1 to 4094. **Note** There is a limit of 200 VLANs per physical interface and 16000 VLANs across the system.

Command Default

None

Command Modes

PVRSTAG interface configuration, PVSTAG interface configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable a VLAN in the PVSTAG configuration mode:

```
RP/0/RSP0/CPU0:router(config)# spanning-tree pvstag A
RP/0/RSP0/CPU0:router(config-pvstag)# interface GigabitEthernet 0/3/03
RP/0/RSP0/CPU0:router(config-pvstag-if)# vlan 100
RP/0/RSP0/CPU0:router(config-pvstag-if-vlan)#
```

Related Commands

Command	Description
debug spanning-tree pvrstag packet, on page 320	Enables packet debugging for sent and received PVRSTAG packets.

Command	Description
debug spanning-tree pvstag packet, on page 322	Enables packet debugging for sent and received PVSTAG packets.
interface (PVSTAG/PVRSTAG), on page 356	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 437	Displays the values currently used for populating the BPDUs sent by all ports.
spanning-tree pvrstag, on page 449	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 451	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.

vlan-ids (MSTAG/REPAG)

To associate a set of VLAN IDs with the current MSTI, use the **vlan-id** command in MSTAG or REPAG instance 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

MSTAG Instance configuration mode, REPAG Instance configuration mode.

Command History

Release	Modification
Release 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RSP0/CPU0:router(config-mstag-inst)# vlan-id 2-1005
```

Related Commands

Command	Description
debug spanning-tree mstag packet, on page 316	Enables MSTAG packet debugging.
debug spanning-tree repag packet, on page 324	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.

Command	Description
interface (MSTAG/REPAG), on page 352	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
instance (MSTAG/REPAG), on page 344	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
spanning-tree mstag, on page 447	Enters the MST Access Gateway configuration submode.
spanning-tree repag, on page 453	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 429	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 439	Displays the values currently used for populating the BPDUs sent by all ports.

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 3.7.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RSP0/CPU0:router(config-mstp-inst)# vlan-id 2-1005
```

Related Commands

Command	Description
debug spanning-tree mst packet, on page 312	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 314	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
instance (MSTP), on page 346	Enters the multiple spanning tree instance (MSTI) configuration submode.

Command	Description
spanning-tree mst, on page 445	Enters the MSTP configuration submode
show spanning-tree mst, on page 414	Displays the multiple spanning tree protocol status information.

Layer 2 Access List Commands

For detailed information about Ethernet services ACL concepts, configuration tasks, and examples, see the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*.

copy access-list ethernet-service

To create a copy of an existing Ethernet services access list, use the **copy access-list ethernet-services** command in EXEC mode.

copy access-list ethernet-service *source-acl destination-acl*

Syntax Description

source-acl	Name of the access list to be copied.
destination-acl	Name of the destination access list where the contents of the *source-acl* argument is copied.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **copy access-list ethernet-service** command to copy a configured Ethernet services access list. Use the *source-acl* argument to specify the access list to be copied and the *destination-acl* argument to specify where to copy the contents of the source access list. The *destination-acl* argument must be a unique name; if the *destination-acl* argument name already exists for an access list, the access list is not copied. The **copy access-list ethernet-service** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists.

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

In the following example, a copy of access list list-1 is created as list-2:

```
RP/0/RSP0/CPU0:router# show access-list ethernet-service list-1

ethernet service access-list list-1
  10 permit any any
  20 permit 2.3.4 5.4.3
RP/0/RSP0/CPU0:router# copy access-list ethernet-service list-1 list-2
RP/0/RSP0/CPU0:router# show access-list ethernet-service list-2
ethernet service access-list list2
  10 permit any any
  20 permit 2.3.4 5.4.3
```

Related Commands

Command	Description
deny (ES ACL), on page 466	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 469	Controls access to an interface.
ethernet-services access-list, on page 471	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 473	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 476	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 478	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 482	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 484	Identifies the modes and interfaces on which a particular ACL is applied.

deny (ES ACL)

To set conditions for an Ethernet services access list, use the **deny** command in Ethernet services access list configuration mode. To remove a condition, use the **no** form of the command.

[*sequence-number*] **deny** {*src-mac-address src-mac-mask*| **any**| **host**| *dest-mac-address dest-mac-mask*} [*ethertype-number*| **capture**| **vlan** *min-vlan-ID* [*max-vlan-ID*]] [**cos** *cos-value*] **[dei]** [**inner-vlan** *min-vlan-ID* [*max-vlan-ID*]] [**inner-cos** *cos-value*] **[inner-dei]**

no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **deny** statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the **resequence access-list ethernet-service** command to change the number of the first statement and increment subsequent statements of a configured access list.
src-mac-address	Source MAC address in format *H.H.H*.
src-mac-mask	Source MAC mask in format *H.H.H*.
any	Denies any source MAC address and mask.
host	Denies host with a specific host source MAC address and mask, in format *H.H.H*.
dest-mac-address	Destination MAC address in format *H.H.H*.
dest-mac-mask	Destination MAC mask in format *H.H.H*.
ethertype-number	16-bit ethertype number in hexadecimal. Range is 0x1 to 0xffff.
capture	(Optional) Captures packets using the traffic mirroring feature and copies this to a capture file.
vlan	(Optional) Denies a specific VLAN or a range of VLANs.
min-vlan-ID	ID for a specific VLAN or the beginning of a range of VLAN IDs.
max-vlan-ID	(Optional) ID for the end of a range of VLAN IDs.
cos	(Optional) Denies based on class of service value.
cos-value	Class of service value. Range is from 0 to 7.
dei	(Optional) Denies based on the setting of the discard eligibility indicator (DEI).

inner-vlan	(Optional) Denies a specific VLAN ID or range of VLAN IDs for the inner header.
min-vlan-ID	ID for a specific VLAN or the beginning of a range of VLAN IDs.
max-vlan-ID	(Optional) ID for the end of a range of VLAN IDs.
inner-cos	(Optional) Denies based on inner header class of service value.
cos-value	Inner header class of service value. Range is from 0 to 7.
inner-dei	(Optional) Denies based on inner header discard eligibility indicator.

Command Default

There is no default condition under which a packet is denied passing the Ethernet services access list.

Command Modes

Ethernet services access list configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **deny** command following the **ethernet-service access-list** command to specify conditions under which a packet can pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit** or **deny** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

If you want to add a statement between two consecutively numbered statements (for example, between lines 10 and 11), first use the resequence access-list ethernet-service, on page 476 command to renumber the first statement and increment the entry number of each subsequent statement.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to define an Ethernet services access list named L2ACL1:

```
RP/0/RSP0/CPU0:router(config)# ethernet-services access-list L2ACL1
RP/0/RSP0/CPU0:router(config-es-acl)# 10 permit 00ff.eedd.0010 ff00.0000.00ff 0011.ab10.cdef
 ffff.0000.ff00 vlan 1000-1100  inner-vlan 100 inner-cos 7 inner-dei
RP/0/RSP0/CPU0:router(config-es-acl)# 20 deny host eedd.0011.ff1c ff00.0000.00ff any vlan
300  cos 1 dei inner-vlan 30 inner-cos 6
RP/0/RSP0/CPU0:router(config-es-acl)# 30 permit any any vlan 500 cos 2 inner-vlan 600
inner-cos 5 inner-dei
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 464	Creates a copy of an existing Ethernet services access list.
ethernet-service access-group, on page 469	Controls access to an interface.
ethernet-services access-list, on page 471	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 473	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 476	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 478	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 482	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 484	Identifies the modes and interfaces on which a particular ACL is applied.

ethernet-service access-group

To control access to an interface, use the **ethernet-service access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of the command.

ethernet-service access-group *access-list-name* {**ingress| egress**}

no ethernet-service access-group *access-list-name* {**ingress| egress**}

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.
egress	Filters on outbound 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 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **ethernet-service access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *acl-name* argument to specify a particular Ethernet services access list. Use the **ingress** keyword to filter on inbound packets or the **egress** keyword to filter on outbound 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 and returns a host unreachable message.

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 show how to apply filters on packets inbound and outbound from GigabitEthernet interface 0/2/0/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ethernet-service access-group p-ingress-filter ingress
RP/0/RSP0/CPU0:router(config-if)# ethernet-service access-group p-egress-filter egress
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 464	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 466	Sets conditions for an Ethernet services access list
ethernet-services access-list, on page 471	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 473	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 476	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 478	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 482	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 484	Identifies the modes and interfaces on which a particular ACL is applied.

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. To remove all entries in an Ethernet services access list, use the **no** form of the command.

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

no 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 3.7.2	This command was introduced.

Usage Guidelines

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

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 with the **deny** (ES ACL) or **permit** (ES ACL) command.

Use the resequence access-list ethernet-service, on page 476 command if you need to add a **permit** or **deny** statement between consecutive entries in an existing Ethernet services access lists.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to define an Ethernet services access list named L2ACL1:

```
RP/0/RSP0/CPU0:router(config)# ethernet-services access-list L2ACL1
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 464	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 466	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 469	Controls access to an interface.
permit (ES ACL), on page 473	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 476	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 478	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 482	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 484	Identifies the modes and interfaces on which a particular ACL is applied.

permit (ES ACL)

To set conditions for an Ethernet services access list, use the **permit** command in Ethernet services access list configuration mode. To remove a condition, use the **no** form of the command.

[*sequence-number*] **permit** {*src-mac-address src-mac-mask*| **any**| **host**| *dest-mac-address dest-mac-mask*} [*ethertype-number*| **capture**| **vlan** *min-vlan-ID* [*max-vlan-ID*]] [**cos** *cos-value*] **[dei]** [**inner-vlan** *min-vlan-ID* [*max-vlan-ID*]] [**inner-cos** *cos-value*] **[inner-dei]**

no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the **resequence access-list ethernet-service** command to change the number of the first statement and increment subsequent statements of a configured access list.
src-mac-address	Source MAC address in format *H.H.H*.
src-mac-mac	Source MAC mask in format *H.H.H*.
any	Permits any source MAC address and mask.
host	Permits host with a specific host source MAC address and mask, in format *H.H.H*.
dest-mac-address	Destination MAC address in format *H.H.H*.
dest-mac-mac	Destination MAC mask in format *H.H.H*.
ethertype-number	16-bit ethertype number in hexadecimal. Range is 0x1 to 0xffff.
capture	(Optional) Captures packets using the traffic mirroring feature and copies this to a capture file.
vlan	(Optional) Permits a specific VLAN or a range of VLANs.
min-vlan-ID	ID for a specific VLAN or the beginning of a range of VLAN IDs.
max-vlan-ID	(Optional) ID for the end of a range of VLAN IDs.
cos	(Optional) Permits based on class of service value.
cos-value	Class of service value. Range is from 0 to 7.
dei	(Optional) Permits based on the setting of the discard eligibility indicator (DEI).

inner-vlan	(Optional) Permits a specific VLAN ID or range of VLAN IDs for the inner header.
min-vlan-ID	ID for a specific VLAN or the beginning of a range of VLAN IDs.
max-vlan-ID	(Optional) ID for the end of a range of VLAN IDs.
inner-cos	(Optional) Permits based on inner header class of service value.
cos-value	Inner header class of service value. Range is from 0 to 7.
inner-dei	(Optional) Permits based on inner header discard eligibility indicator.

Command Default

There is no specific default condition under which a packet is permitted passing the Ethernet services ACL.

Command Modes

Ethernet services access list configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **permit** command following the **ethernet-service access-list** command to specify conditions under which a packet can pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit** or **deny** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

If you want to add a statement between two consecutively numbered statements (for example, between lines 10 and 11), first use the resequence access-list ethernet-service, on page 476 command to renumber the first statement and increment the entry number of each subsequent statement.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example show how to set a permit condition for an access list named L2ACL1:

```
RP/0/RSP0/CPU0:router(config)# ethernet-services access-list L2ACL1
RP/0/RSP0/CPU0:router(config-es-al)# 10 permit 00ff.eedd.0010 ff00.0000.00ff 0011.ab10.cdef
 ffff.0000.ff00 vlan 1000-1100  inner-vlan 100 inner-cos 7 inner-dei
RP/0/RSP0/CPU0:router(config-es-al)# 20 permit any host 000a.000b.000c 0800 vlan 500 cos 2
 inner-vlan 600 inner-cos 5 inner-dei
RP/0/RSP0/CPU0:router(config-es-al)# 30 permit any host 000a.000b.000c 8137 vlan 500 cos 2
 inner-vlan 600 inner-cos 5 inner-dei
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 464	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 466	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 469	Controls access to an interface.
ethernet-services access-list, on page 471	Defines an Ethernet services (Layer 2) access list by name.
resequence access-list ethernet-service, on page 476	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 478	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 482	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 484	Identifies the modes and interfaces on which a particular ACL is applied.

resequence access-list ethernet-service

To renumber existing statements and increment subsequent statements to allow a new Ethernet services access list statement, use the **resequence access-list ethernet-service** command in EXEC mode.

resequence access-list ethernet-service *access-list-name* [*starting-sequence-number* [*increment*]]

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.
starting-sequence-number	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. Maximum value is 2147483646. Default is 10.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483646. Default is 10.

Command Default

starting-sequence-number: 10

increment: 10

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **resequence access-list ethernet-service** command to add a permit or deny statement between consecutive entries in an existing Ethernet services access list. Specify the first entry number (the *start-sequence-number*) and the increment by which to separate the entry numbers of the statements. the software remembers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

In the following example, suppose you have an existing access list:

```
ethernet service access-list L2ACL1
  10 permit 1.2.3 4.5.6
  20 deny 2.3.4 5.4.3
  30 permit 3.1.2 5.3.4 cos 5
```

You need to add additional entries in the access list ahead of the first permit statement. First, you resequence the entries, renumbering the statements starting with number 20 and an increment of 10, and then you have room for additional statements between each of the existing statements:

```
RP/0/RSP0/CPU0:router# resequence access-list ethernet-service L2ACL1 20 10
RP/0/RSP0/CPU0:router# show access-list ethernet-services L2ACL1

ethernet service access-list L2ACL1
  20 permit 1.2.3 4.5.6
  30 deny 2.3.4 5.4.3
  40 permit 3.1.2 5.3.4 cos 5
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 464	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 466	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 469	Controls access to an interface.
ethernet-services access-list, on page 471	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 473	Sets conditions for an Ethernet services access list.
show access-lists ethernet-services, on page 478	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 482	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 484	Identifies the modes and interfaces on which a particular ACL is applied.

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*| **maximum**| **standby**| **summary**] [**hardware**| **usage**] [**ingress**| **egress**] [**implicit**| **detail**| **sequence**| **location** *location*]

Syntax Description

access-list-name	(Optional) Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
maximum	(Optional) Show the maximum number of configurable Ethernet services ACLs and ACEs.
standby	(Optional) Display all access lists in standby mode.
summary	(Optional) Display a summary of Ethernet services access lists.
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.
usage	(Optional) Display the usage of this ACL in a given location.
ingress	(Optional) Filters on inbound packets.
egress	(Optional) Filters on outbound packets.
implicit	(Optional) Display the count of packets implicitly denied by a particular ACL.
detail	(Optional) Display TCAM entries.
sequence	(Optional) Display statistics for a specific sequence number.
sequence-number	Sequence number value. Range is 1 to 2147483647.
location	(Optional) Display information for a specific node number.
location	Fully qualified location specification

Command Default

The contents of all Ethernet services access lists are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
acl	read, write

Examples

The following examples lists defined Ethernet services access list maximum thresholds:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services maximum

  Max configurable ACLs: 10000
  Max configurable ACEs: 350000

RP/0/RSP0/CPU0:router# show access-lists ethernet-services maximum detail

  Total ACLs configured: 2
  Total ACEs configured: 3
  Max configurable ACLs: 10000
  Max configurable ACEs: 350000
```

The following example lists the Ethernet services access-list standby:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services standby

ethernet-services access-list i
 10 permit host 0001.0002.0003 host 000a.000b.000c
ethernet-services access-list l2_acl
 10 permit any any
 20 deny host 0002.0003.0004 host 000.50004.0003
```

The following example displays a summary of the number of Ethernet services ACLs configured on the system:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services summary

ACL Summary:
  Total ACLs configured: 2
  Total ACEs configured: 3
```

The following example displays the number of packets matching the access list l2_acl for each ACE:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services l2_ACL hardware ingress location
 0/0/CPU0

ethernet service access-list l2_acl
  10 permit any any ( 3524 hw matches)
  20 deny host 0002.0003.0004 host 0005.0004.0003 (5394 hw matches)
```

The following example displays the number of packets matching the implicit deny in access list l2_acl:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services l2_ACL hardware ingress implicit
 location 0/0/CPU0

ethernet-services access-list l1_acl
 2147483647 implicit deny any any (2300 hw matches)
```

The following example displays the number of packets matching a particular sequence number:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services l2_ACL hardware ingress sequence
 20 location 0/0/CPU0

ethernet-services access-list l2_acl
 20 deny host 0002.0003.0004 host 0005.0004.0003 (5394 hw matches)
```

The following example displays statistics for the TCAM entry for Ethernet services access list l2acl_4:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services l2acl_4 hardware ingress sequence
 10 detail location 0/6/CPU0
Wed Jun 24 00:28:51.367 UTC

ACL name: l2acl_4
Format type : 1
Channel ID: 2
Sequence Number: 10
Grant: permit
Logging: OFF
Hits: 0
Statistics pointer: 0x150628
Number of TCAM entries: 1
idx = 0
Entry : 0 for ACE : 10
RAW value  : 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
RAW mask   : 00 03 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

-------------------------------Field Details----------------------------------
outer_vlan_id value     : 0000
outer_vlan_id mask      : 0ffff
outer_vlan discard eligibility value: 00
outer_vlan discard eligibility mask : 01
outer_vlan_id cos value: 00
outer_vlan_id cos mask: 07
Ethernet type value     : 0000
Ethernet type mask      : ffff
Base app id value     : 02
Base app id value     : 00
Base acl id value    : 0001
Base acl id mask     : 0000
outer vlan id present value     : 0
outer vlan id present mask      : 1
inner vlan id present value     : 0
inner vlan id present mask      : 1
Mac source address value     : 0000 0000 0000
Mac source address mask      : ffff ffff ffff
Mac destination address value  : 0000 0000 0000
Mac destination address mask   : ffff ffff ffff
RP/0/RSP0/CPU0:router#
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 464	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 466	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 469	Controls access to an interface.

Command	Description
ethernet-services access-list, on page 471	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 473	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 476	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services trace, on page 482	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 484	Identifies the modes and interfaces on which a particular ACL is applied.

show access-lists ethernet-services trace

To display Ethernet services access list trace information use the **show access-lists ethernet-services trace** command in EXEC mode.

show access-lists ethernet-services trace {**client**| **intermittent**| **critical**| **both**| **all**}

Syntax Description

client	Trace data for ES ACL client.
intermittent	Trace data for intermittent failures.
critical	Trace data for server-critical failures
both	Trace data for server-critical and intermittent failures.
all	Trace data for server-critical and intermittent failures.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
acl	read

Examples

The following examples show how to display Ethernet services access list trace information:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services trace all
1 unique entries (256 possible, 0 filtered)
Jun 15 06:42:56.980 es/acl_mgr_un 0/RSP0/CPU0 1#t3 Manager state is active
3 wrapping entries (1024 possible, 0 filtered, 3 total)
Jun 15 06:42:57.053 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:23:30.075 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:29:41.383 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
```

```
 2 batches

RP/0/RSP0/CPU0:router# show access-lists ethernet-services trace both
1 unique entries (256 possible, 0 filtered)
Jun 15 06:42:56.980 es/acl_mgr_un 0/RSP0/CPU0 1#t3 Manager state is active
3 wrapping entries (1024 possible, 0 filtered, 3 total)
Jun 15 06:42:57.053 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:23:30.075 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:29:41.383 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 2 batches

RP/0/RSP0/CPU0:router# show access-lists ethernet-services trace critical
1 unique entries (256 possible, 0 filtered)
Jun 15 06:42:56.980 es/acl_mgr_un 0/RSP0/CPU0 1#t3 Manager state is active

RP/0/RSP0/CPU0:router# show access-lists ethernet-services trace intermittent
3 wrapping entries (1024 possible, 0 filtered, 3 total)
Jun 15 06:42:57.053 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:23:30.075 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:29:41.383 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 2 batches
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 464	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 466	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 469	Controls access to an interface.
ethernet-services access-list, on page 471	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 473	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 476	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 478	Displays the contents of current Ethernet services access lists.
show access-list ethernet-service usage pfilter, on page 484	Identifies the modes and interfaces on which a particular ACL is applied.

show access-list ethernet-service usage pfilter

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

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

Syntax Description

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

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
acl	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# show access-list ethernet-services usage pfilter location 0/0/cpu0
pfilter location 0/0/cpu0
Interface : GigabitEthernet0/0/0/9
    Input ACL : l2_acl
    Output ACL : N/A
Interface : GigabitEthernet0/0/0/30
```

```
    Input ACL : N/A
    Output ACL : i
```

The following example shows the results of the command for a specific ACL:

```
RP/0/RSP0/CPU0:router# show access-list ethernet-services l2_acl usage pfilter location
0/0/CPU0
Interface : GigabitEthernet0/0/0/9
    Input ACL : l2_acl
    Output ACL : N/A
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 464	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 466	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 469	Controls access to an interface.
ethernet-services access-list, on page 471	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 473	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 476	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 478	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 482	Displays Ethernet services access list trace information.

show lpts pifib hardware entry optimized

To display a set of optimized entries that are combined as a single entry, inside the Ternary Content Addressable Memory (TCAM), use the **show lpts pifib hardware entry optimized** command in EXEC mode.

show lpts pifib hardware entry optimized *location*

Syntax Description

location	Mandatory. The location of the line card where the interface is present.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
lpts	read

Examples

The following example shows the output of the **show lpts pifib hardware entry optimized**command:

```
RP/0/RSP0/CPU0:router# show lpts pifib hardware entry optimized location 0/4/CPU0
Node: 0/4/CPU0:
----------------------------------------
Protocol - Layer4 Protocol; Intf - Interface in optimized list

Protocol   laddr.Port, raddr.Port    Intf            VRF id       State
---------- ------------------------- --------------- ------------ --------------------
IGMP       224.0.0.22.any , any.any  Te0/4/0/0       *            Uidb Set
                                     Te0/4/0/1       *            Uidb Set

           224.0.0.22.any , any.any  Te0/4/0/0       *            Uidb Set
                                     Te0/4/0/1       *            Uidb Set

           any.any , any.any         Te0/4/0/0       *            Uidb Set
                                     Te0/4/0/1       *            Uidb Set
```

INDEX