Cisco IOS XR Virtual Private Network Command Reference for the Cisco XR 12000 Series Router, Release 4.1

First Published: March 14, 2011

Last Modified: March 14, 2011

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

CONTENTS

Preface

The *Cisco IOS XR Virtual Private Network Command Reference for the Cisco XR 12000 Series Router* preface contains these sections:

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.

Virtual Private Network Commands

For detailed information about virtual private network concepts, configuration tasks, and examples, refer to the *Cisco IOS XR Virtual Private Network Configuration Guide for the Cisco XR 12000 Series Router*

authentication (L2TP)

To enable L2TP authentication for a specified L2TP class name, use the **authentication** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

authentication

no authentication

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

L2TP class configuration

Command History

Release	Modification
Release 3.7.0	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 You can also enable L2TP authentication for a specified class name from L2TP class configuration submode. To enter this submode, enter the **l2tp-class** command followed by the class name.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure L2TP authentication for the specified L2TP class name "cisco":

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)# authentication
```

Related Commands

Command	Description
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.

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 3.8.0	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.

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

Related Commands

Command	Description
backup disable (L2VPN), on page 7	Specifies how long a backup pseudowire should wait before resuming operation after the primary pseudowire goes down.
l2vpn, on page 47	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 53	Configures a pseudowire for a cross-connect.
p2p, on page 63	Enters p2p configuration submode to configure point-to-point cross-connects.
xconnect group, on page 110	Configures cross-connect groups.

backup disable (L2VPN)

To specify how long a backup pseudowire should wait before resuming operation after the primary pseudowire goes down, 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 primary pseudowire becomes nonfunctional before the Cisco IOS XR software attempts to activate the secondary 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 3.8.0	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, 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# pw-class class1
RP/0/0/CPU0:router(config-l2vpn-pwc)# backup disable delay 50
RP/0/0/CPU0:router(config-l2vpn-pwc)# exit
RP/0/0/CPU0:router(config-l2vpn)# xconnect group A
RP/0/0/CPU0:router(config-l2vpn-xc)# p2p rtrx
RP/0/0/CPU0:router(config-l2vpn-xc-p2p)# neighbor 10.1.1.1 pw-id 2
RP/0/0/CPU0:router(config-l2vpn-xc-p2p-pw)# pw-class class1
RP/0/0/CPU0:router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
RP/0/0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)#
```

Related Commands

Command	Description
l2vpn, on page 47	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 53	Configures a pseudowire for a cross-connect.
p2p, on page 63	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 57	Enters pseudowire class submode to define a pseudowire class template.
xconnect group, on page 110	Configures cross-connect groups.

clear l2tp counters control session

To clear L2TP control counters for a session, use the **clear l2tp counters control session** command in EXEC mode.

clear l2tp counters control session fsm [**event**| **state transition**]

Syntax Description

fsm	(Optional) Clears finite state machine counters.
event	(Optional) Clears state machine event counters.
state	(Optional) Clears state machine state counters.
transition	(Optional) Clears state machine transition counters.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 all L2TP state machine transition counters:

```
RP/0/0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)## clear l2tp counters control session fsm
 state transition
```

Related Commands

Command	Description
clear l2tp counters control tunnel, on page 11	Clears L2TP control counters for a tunnel.
clear l2vpn counters l2tp, on page 16	Clears L2VPN statistical information, such as, packets dropped.

clear l2tp counters control tunnel

To clear L2TP control counters for a tunnel, use the **clear l2tp counters control tunnel** command in EXEC mode.

clear l2tp counters control tunnel {**all**| **authentication**| **id** *tunnel id*}

Syntax Description

all	Clears all L2TP counters, except authentication counters
authentication	Clears tunnel authentication counters.
id *tunnel id*	Clears a specified counter. Range is 1 to 4294967295.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 all L2TP control tunnel counters:

```
RP/0/0/CPU0:router# clear l2tp counters control tunnel all
```

Related Commands

Command	Description
clear l2tp counters control session, on page 9	Clears L2TP control counters for a session.

Command	Description
clear l2vpn counters l2tp, on page 16	Clears L2VPN statistical information, such as, packets dropped.

clear l2tp tunnel

To clear L2TP tunnels, use the **clear l2tp tunnel** command in EXEC mode.

clear l2tp tunnel {**all**| **id** *tunnel id*| **l2tp-class** *class name*| **local ipv4** *ipv4 address*| **remote ipv4** *ipv4 address*}

Syntax Description

all	Clears all L2TP tunnels.
id *tunnel id*	Clears a specified tunnel.
l2tp-class *class name*	Clears all L2TP tunnels based on L2TP class name.
local ipv4 *ipv4 address*	Clears all local tunnels based on the specified local IPv4 address.
remote ipv4 *ipv4 address*	Clears all remote tunnels based on the specified local IPv4 address.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 all L2TP tunnels:

```
RP/0/0/CPU0:router# clear l2tp tunnel all
```

Related Commands

Command	Description
clear l2tp counters control session, on page 9	Clears L2TP control counters for a session.
clear l2tp counters control tunnel, on page 11	Clears L2TP control counters for a tunnel.

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 3.4.0	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 change counters for L2VPN collaborators:

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

Related Commands

Command	Description
show l2vpn collaborators, on page 81	Displays information about the state of the interprocess communications connections between l2vpn_mgr and other processes.

clear l2vpn counters l2tp

To clear L2VPN statistical information, such as, packets dropped, use the **clear l2vpn counters l2tp** command in EXEC mode.

clear l2vpn counters l2tp [**neighbor** *ip-address* [**pw-id** *value*]]

Syntax Description

l2tp	Clears all L2TP counters.
neighbor *ip-address*	(Optional) Clears all L2TP counters for the specified neighbor.
pw-id *value*	(Optional) Configures the pseudowire ID. The range is from 1 to 4294967295.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.7.0	The **pw-id** 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 clear all L2TP counters:

```
RP/0/0/CPU0:router# clear l2vpn counters l2tp
```

Related Commands

Command	Description
show l2vpn collaborators, on page 81	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 3.7.0	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 the MAC withdrawal statistics over all the bridges:

```
RP/0/0/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 3.4.0	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 L2VPN forwarding counters:

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

Related Commands

Command	Description
show l2vpn forwarding, on page 83	Displays forwarding information from the layer2_fib manager on the line card.

clear l2vpn forwarding mac-address-table

To clear L2VPN forwarding MAC address tables, use the **clear l2vpn forwarding mac-address-table** command in EXEC mode.

clear l2vpn forwarding mac-address-table {**address** *address*| **bridge-domain name**| **interface** *type interface-path-id*| **location** *node-id*}

Syntax Description

address	Clears a specified MAC address.
bridge-domain *name*	Clears bridge domains learned from a MAC address table.
type	(Optional) 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 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*	Clears L2VPN forwarding message counters 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 3.5.0	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, execute

Examples

The following example shows how to clear L2VPN forwarding MAC address tables on a specified node:

```
RP/0/0/CPU0:router# clear l2vpn forwarding mac-address location 1/1/1
```

Related Commands

Command	Description
show l2vpn forwarding, on page 83	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 3.5.0	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 L2VPN forwarding message counters on a specified node:

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

Related Commands

Command	Description
show l2vpn forwarding, on page 83	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 3.4.0	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/0/0/CPU0:router# clear l2vpn forwarding table location 1/2/3/5
```

Related Commands

Command	Description
show l2vpn forwarding, on page 83	Displays forwarding information from the layer2_fib manager on the line card.

digest (L2TP)

To configure digest options, use the **digest** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

digest {**check disable**| **hash** {**MD5**| **SHA1**}| **secret** {**0**| **7**| *word*}}

no digest {**check disable**| **hash** {**MD5**| **SHA1**}| **secret** {**0**| **7**| *word*}}

Syntax Description

check disable	Disables digest checking.
hash {**MD5** | **SHA1**}	Configures the digest hash method (MD5 or SHA1). Default is MD5.
secret {**0** | **7** | *word*}	Configures a shared secret for message digest.

Command Default

check disable: Digest checking is enabled by default.

hash: Default is MD5 if the **digest** command is issued without the secret keyword option and L2TPv3 integrity checking is enabled.

Command Modes

L2TP class configuration

Command History

Release	Modification
Release 3.7.0	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 digest secret and hash algorithm can be configured in the l2tp-class configuration for authentication of the control channel. For control channel authentication to work correctly, however, both sides of the L2TP control channel connection must share a common secret and hash algorithm.

To update of digest secret without network disruption, Cisco supports a maximum to two digest secrets. You can configure a new secret while keeping the old secret valid. You can safely remove the old secret after you update all affected peer nodes with a new secret,

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure digest options for L2TP:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)# digest check disable
RP/0/0/CPU0:router(config-l2tp-class)# digest secret cisco hash md5
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.

hello-interval (L2TP)

To configure the hello-interval value for L2TP (duration between control channel hello packets), use the **hello interval (L2TP)** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

hello-interval *interval*

no hello-interval *interval*

Syntax Description

interval	Interval (in seconds) between control channel hello packets. The range is from 0 to 1000. Default is 60 seconds.

Command Default

interval: 60 seconds

Command Modes

L2TP class configuration

Command History

Release	Modification
Release 3.7.0	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 the hello-interval value for L2TP to 22 seconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)# hello-interval 22
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.

Command	Description
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.

hidden (L2TP)

To enable hidden attribute-value pairs (AVPs), use the **hidden** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

hidden

no hidden

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

L2TP class configuration

Command History

Release	Modification
Release 3.7.0	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 enable hidden AVPs:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)# hidden
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.

Command	Description
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.

hostname (L2TP)

To define the name used in the L2TP hostname AVP, use the **hostname** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

hostname *name*

no hostname *name*

Syntax Description

name	Hostname used to identify the router during L2TP control channel authentication.

Command Default

None

Command Modes

L2TP class configuration

Command History

Release	Modification
Release 3.7.0	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 hostname using the word “cisco”:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)# hostname cisco
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).

Command	Description
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.

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 3.4.0	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 an attachment circuit on a TenGigE interface:

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

Related Commands

Command	Description
p2p, on page 63	Enters p2p configuration submode to configure point-to-point cross-connects.

l2tp-class

To enter L2TP class configuration mode where you can define an L2TP signaling template, use the **l2tp-class** command in global configuration mode. To delete the L2TP class, use the **no** form of this command.

l2tp-class *l2tp-class-name*

no l2tp-class *l2tp-class-name*

Syntax Description

l2tp-class-name	L2TP class name.

Command Default

No L2TP classes are defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.0	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 An L2TP class name must be defined before configuring L2TP control plane configuration settings.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enter L2TP configuration mode to create a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes (in this case, the word “cisco” is used):

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)#
```

l2tp-class configuration

To enter L2TP class configuration mode in which an L2TP signaling template is not defined, use the **l2tp-class configuation** command in global configuration mode. To delete the L2TP class configuration, use the **no** form of this command.

l2tp-class configuration

no l2tp-class configuration

Syntax Description

This command has no arguments or keywords.

Command Default

No L2TP classes are defined.

Command Modes

Global configuration

Command History

Release	Modification
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, write

Examples

The following example shows how to enter L2TP configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class configuration
RP/0/0/CPU0:router(config-l2tp-class)#
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).

Command	Description
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.

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 3.4.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/0/CPU0:router(config-if)# l2transport
```

Ethernet VLAN Mode:

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

Ethernet VLAN Mode (QinQ):

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

Ethernet VLAN Mode (QinAny):

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

Related Commands

Command	Description
show l2vpn forwarding, on page 83	Displays forwarding information from the layer2_fib manager on the line card.

l2transport cell-packing

To configure L2VPN cell packing parameters, use the **l2transport cell-packing** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

l2transport cell-packing *maximum timer*

no l2transport cell-packing *maximum timer*

Syntax Description

maximum	Maximum number of cells to be packed in a packet. Range is 2 to 86.
timer	Cell packing timer (1, 2, or 3).

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.5.0	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
atm	read, write

Examples

The following example shows how to configure L2VPN cell packing parameters:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/0/CPU0:router(config-if)# l2transport cell-packing 33 2
```

Related Commands

Command	Description
show l2vpn forwarding, on page 83	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 {**cdp**| **pvst**| **stp**| **vtp**} {**drop**| **experimental** *bits*| **tunnel experimental** *bits*}

no l2transport l2protocol {**cdp**| **pvst**| **stp**| **vtp**} {**drop**| **experimental** *bits*| **tunnel experimental** *bits*}

Syntax Description

cdp	Configures Cisco Discovery Protocol (CDP).
pvst	Configures Per VLAN Spanning Tree protocol (PVST).
stp	Configures Spanning Tree Protocol (STP).
vtp	Configures VLAN Trunk Protocol (VTP).
drop	Drops the selected protocol packets.
experimental *bits*	Modifies the MPLS experimental bits.
tunnel experimental *bits*	Configures tunnel protocol packets.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.5.0	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.

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

Related Commands

Command	Description
show l2vpn forwarding, on page 83	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 3.9.0	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 **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

To display the state of l2transport events, use the show controller internal command in *Cisco IOS XR Interface and Hardware Component Configuration Guide for the Cisco XR 12000 Series Router*

For more information about the Ethernet remote port shutdown feature, see *Cisco IOS XR MPLS Configuration Guide for the Cisco XR 12000 Series Router*.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

Related Commands

Command	Description
show l2vpn forwarding, on page 83	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 3.5.0	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
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 83	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 3.4.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)#
```

Related Commands

Command	Description
show l2vpn forwarding, on page 83	Displays forwarding information from the layer2_fib manager on the line card.

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 3.5.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# logging pseudowire status
```

Related Commands

Command	Description
l2vpn, on page 47	Enters L2VPN 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 3.7.0	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 static labels for MPLS L2VPN:

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

Related Commands

Command	Description
l2vpn, on page 47	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 53	Configures a pseudowire for a cross-connect.
p2p, on page 63	Enters p2p configuration submode to configure point-to-point cross-connects.
xconnect group, on page 110	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.

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	The **vccv disable** keyword was added.
Release 3.7.0	The following keywords were removed: • **control-word** • **pw-static-label local** • **remote** • **vccv** • **transport-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.

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 a neighbor only.

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

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

Related Commands

Command	Description
l2vpn, on page 47	Enters L2VPN configuration mode.
p2p, on page 63	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 57	Enters pseudowire class submode to define a pseudowire class template.
xconnect group, on page 110	Configures cross-connect groups.

password (L2TP)

To define the password and password encryption type for control channel authentication, use the **password** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

password [**0**| **7**] *password*

no password

Syntax Description

0	(Optional) Specifies that an unencrypted password will follow.
7	(Optional) Specifies that an encrypted password will follow.
password	Unencrypted or clear text user password.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.0	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 define an unencrypted password using the word “cisco” for control channel authentication:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class sanjose
RP/0/0/CPU0:router(config-l2tp-class)# password 0 cisco
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.

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 3.5.0	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 a simple pseudowire class template:

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

Related Commands

Command	Description
p2p, on page 63	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*]

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 3.7.0	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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/0/CPU0:router(config-l2vpn-pwc)# encapsulation l2tpv3
```

Related Commands

Command	Description
pw-class (L2VPN), on page 57	Enters pseudowire class submode to define a pseudowire class template.
pw-class encapsulation mpls, on page 61	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**| **preferred-path**| **protocol ldp**| **sequencing**| **tag-rewrite**| **transport-mode**| **vccv verification-type none**}

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

Syntax Description

class-name	Encapsulation class name.
control word	Disables control word for MPLS encapsulation. Disabled by default.
ipv4	Sets the local source IPv4 address.
load-balancing	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.
sequencing	Configures sequencing on receive or transmit.
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 3.5.0	This command was introduced.
Release 3.8.0	The keywords **control word disable** and **vccv none** were replaced by the keywords **control word** and **vccv verification-type none** .
Release 3.9.0	The following keywords were added: • **preferred-path** • **sequencing** • **tag-rewrite** • **transport-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.

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

Related Commands

Command	Description
pw-class (L2VPN), on page 57	Enters pseudowire class submode to define a pseudowire class template.
pw-class encapsulation l2tpv3, on page 59	Configures L2TPv3 pseudowire encapsulation.

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 3.4.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# xconnect group group 1
RP/0/0/CPU0:router(config-l2vpn-xc)# p2p xc1
```

Related Commands

Command	Description
interface (p2p), on page 32	Configures an attachment circuit.

receive-window (L2TP)

To configure the receive window size for the L2TP server, use the **receive-window** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

receive-window *size*

no receive-window *size*

Syntax Description

size	Maximum number of packets that are received from a peer before back-off is applied. Default is 512.

Command Default

size: 512

Command Modes

L2TP class configuration

Command History

Release	Modification
Release 3.7.0	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 the receive window size for the L2TP server to 10 packets:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)# receive-window 10
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.

Command	Description
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.

retransmit (L2TP)

To configure retransmit retry and timeout values, use the **retransmit** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

retransmit {**initial** *initial-retries*| **retries** *retries*| **timeout** {**max**| **min**} *timeout*}

no retransmit {**initial** *initial-retries*| **retries** *retries*| **timeout** {**max**| **min**} *timeout*}

Syntax Description

initial *initial-retries*	Configures the number of SCCRQ messages resent before giving up on a particular control channel. Range is 1 to 1000. Default is 2.
retries *retries*	Configures the maximum number of retransmissions before determining that peer router does not respond. Range is 5 to 1000. Default is 15.
timeout {**max** | **min**} *timeout*	Configures the maximum and minimum retransmission interval in seconds for control packets. Range is 1 to 8. Maximum timeout default is 8 seconds. Minimum timeout default is 1 second.

Command Default

initial retries: 2

retries: 15

min timeout: 1

max timeout: 8

Command Modes

L2TP class configuration

Command History

Release	Modification
Release 3.7.0	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 retransmit retry value to 1:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)# retransmit initial retries 1
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.

rollover (L3VPN)

To configure rollover times for a tunnel-template, use the **rollover** command in tunnel encapsulation l2tp configuration mode. To return to the default behavior, use the **no** form of this command.

rollover periodic *time* **holdown** *time*

no rollover periodic *time* **holdown** *time*

Syntax Description

periodic *time*	Configures the periodic rollover time in seconds. Range is 60 to 31536000.
holddown*time*	Configures the holddown time for old session cookie values.

Command Default

None

Command Modes

tunnel encapsulation l2tp configuration

Command History

Release	Modification
Release 3.5.0	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 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 how to configure rollover times for a tunnel-template:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# tunnel-template kanata_9
RP/0/0/CPU0:router(config-tuntem) encapsulation l2tp
RP/0/0/CPU0:router(config-tunencap-l2tp)# rollover
```

Related Commands

Command	Description
interface (p2p), on page 32	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 3.5.0	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.

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

Related Commands

Command	Description
pw-class (L2VPN), on page 57	Enters pseudowire class submode to define a pseudowire class template.

show l2tp class

To display information about an L2TP class, use the **show l2tp class** command in EXEC mode.

show l2tp class name *name*

Syntax Description

name *name*	Configures an L2TP class name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 sample output for the **show l2vtp session class** command:

```
RP/0/0/CPU0:router# show l2tp class name kanata_02

l2tp-class kanata_02
  manually configured class
  configuration parameters:
     (not) hidden
     (no) authentication
     (no) digest
     digest check enable
     hello 60
     (no) hostname
     (no) password
     (no) accounting
     (no) security crypto-profile
     (no) ip vrf
     receive-window 888
     retransmit retries 15
```

```
    retransmit timeout max 8
    retransmit timeout min 1
    retransmit initial retries 2
    retransmit initial timeout max 8
    retransmit initial timeout min 1
    timeout setup 300
```

This table describes the significant fields shown in the display.

Table 1: show l2tp class brief Field Descriptions

Field	Description
l2tp-class	Shows the L2TP class name and the manner of its creation. For example, manually configured class.
configuration parameters	Displays a complete list and state of all configuration parameters.

Related Commands

Command	Description
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.

show l2tp counters forwarding session

To display L2TP forward session counters, use the **show l2tp counter forwarding session** command in EXEC mode.

show l2tp counters forwarding session [**id** *identifier*| **name** *local-name remote-name*]

Syntax Description

id *identifier*	(Optional) Configures the session counter identifier.
name *local-name remote name*	(Optional) Configures the local and remote names for a session counter.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 sample output for the **show l2tp counters forwarding session** command:

```
RP/0/RP00/CPU0:router(config-l2vpn)# pw-class kanata01show l2tp counters forwarding session

LocID       RemID       TunID       Pkts-In     Pkts-Out    Bytes-In    Bytes-Out
22112       15584       14332             0            0           0            0
```

This table describes the significant fields shown in the display.

Table 2: show l2tp counters forwarding session Field Descriptions

Field	Description
LocID	Local session ID.
RemID	Remote session ID.
TunID	Local Tunnel ID for this session.
Pkts-In	Number of packets input in the session.
Pkts-Out	Number of packets output in the session.
Bytes-In	Number of bytes input in the session.
Bytes-Out	Number of bytes output in the session.

Related Commands

Command	Description
show l2tp tunnel, on page 79	Displays information about L2TP tunnels.

show l2tp session

To display information about L2TP sessions, use the **show l2tp session** command in EXEC mode.

show l2tp session [**detail**| **brief**| **interworking**| **circuit**| **sequence**| **state**] {**id** *id*| **name** *name*}

Syntax Description

brief	(Optional) Displays summary output for a session.
circuit	(Optional) Displays attachment circuit information for a session.
detail	(Optional) Displays detailed output for a session.
interworking	(Optional) Displays interworking information for a session.
sequence	(Optional) Displays data packet sequencing information for a session.
state	(Optional) Displays control plane state information for a session.
id *id*	Configures the local tunnel ID. Range is 0 to 4294967295.
name *name*	Configures the tunnel name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 sample output is from the **show l2vtp session brief** command:

```
RP/0/RP00/CPU0:router(config-l2vpn-pw)# encapsulation mplsshow l2tp session brief

L2TP Session Information Total tunnels 1 sessions 6

LocID      TunID      Peer-address    State     Vcid
                                      sess/cir
26093      43554      13.0.0.2        est,UP     60
26094      43554      13.0.0.2        est,UP     40
26095      43554      13.0.0.2        est,UP     50
26096      43554      13.0.0.2        est,UP     70
26097      43554      13.0.0.2        est,UP     20
26098      43554      13.0.0.2        est,UP     30
```

This table describes the significant fields shown in the display.

Table 3: show l2tp session brief Field Descriptions

Field	Description
LocID	Local session ID.
TunID	Local tunnel ID for this session.
Peer-address	The IP address of the other end of the session.
State	The state of the session.
Vcid	The Virtual Circuit ID of the session. This is the same value of the pseudowire ID for l2vpn.

Related Commands

Command	Description
show l2tp tunnel, on page 79	Displays information about L2TP tunnels.

show l2tp tunnel

To display information about L2TP tunnels, use the **show l2tp tunnel** command in EXEC mode.

show l2tp tunnel {**detail**| **brief**| **state**| **transport**} {**id** *identifier*| **name** *local-name remote-name*}

Syntax Description

detail	Displays detailed output for L2TP tunnels.
brief	Displays summary information for the tunnel.
state	Displays control plane state information.
transport	Displays transport information (IP) for each selected control channel.
id *identifier*	Displays local control channel identifiers.
name *local-name remote-name*	Displays the local and remote names of a control channel.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 sample output is from the **show l2tp tunnel** command:

```
RP/0/0/CPU0:router(config-l2vpn-encap-mpls)# sequencing bothshow l2tp tunnel

L2TP Tunnel Information Total tunnels 1 sessions 6
```

```
LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class
43554 6220  PE2           est    13.0.0.2        0     6        foo
```

This table describes the significant fields shown in the display.

Table 4: show l2tp tunnel Field Descriptions

Field	Description
LocID	Local session ID.
RemID	Remote session ID.
Remote Name	Remote name of the session.
State	State of the session.
Remote Address	Remote address of the session.
Port	Session port.
Sessions	Number of sessions.
L2TP	L2TP class name.

Related Commands

Command	Description
show l2tp session, on page 77	Displays information about L2TP sessions.

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 3.4.0	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 sample output for the **show l2vpn collaborators** command:

```
RP/0/0/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 5: 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 15	Clears the state change counters for L2VPN collaborators.

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**| **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.
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 3.4.0	This command was introduced.
Release 3.7.0	Sample output was updated to add MAC information for the layer2_fib manager summary.

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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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
```

Related Commands

Command	Description
clear l2vpn forwarding counters, on page 19	Clears L2VPN forwarding counters.

show l2vpn forwarding l2tp

To display L2VPN forwarding information, use the **show l2vpn forwarding l2tp** command in EXEC mode.

show l2vpn forwarding l2tp disposition {**local session id** *session-ID*| **hardware**| **location** *node-id*} **location** *node-id*

Syntax Description

disposition	Displays forwarding disposition information.
session-ID	Displays L2TPv3-related forwarding information for the specified local session ID. Range is 1-4294967295.
hardware	Displays L2TPv3-related forwarding information read from hardware.
location	Displays L2TPv3-related forwarding information for the specified location.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 example shows sample output for the **show l2vpn forwarding l2tp** command:

```
RP/0/0/CPU0:router# show l2vpn forwarding l2tp disposition hardware location 0/3/1

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

Related Commands

Command	Description
clear l2vpn forwarding counters, on page 19	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 3.5.0	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 example shows sample output for the **show l2vpn pw-class** command:

```
RP/0/0/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 6: 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 19	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 3.4.0	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 example shows sample output for the **show l2vpn resource** command:

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

Memory: Normal
```

describes the significant fields shown in the display.Table 7: show l2vpn resource Command Field Descriptions, on page 92

Table 7: 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 [**detail**| **group**| **interface**| **neighbor**| **state**| **summary**| **type**| **state unresolved**]

Syntax Description

detail	(Optional) Displays detailed information.
group	(Optional) Displays all cross-connects in a specified group.
interface	(Optional) Filters the interface and subinterface.
neighbor	(Optional) Filters the neighbor.
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
state unresolved	(Optional) Displays information about unresolved cross-connects.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.4.1	VCCV-related show command output was added.
Release 3.6.0	Preferred-path-related show command output was added.

Release	Modification
Release 3.7.0	Sample output was updated to display the backup pseudowire information.

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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/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 table describes the significant fields shown in the display.

Table 8: 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 110	Configures cross-connect groups.

show tunnel-template

To display tunnel template information, use the **show tunnel-template** command in the EXEC mode.

show tunnel-template *template-name*

Syntax Description

template-name	Name of the tunnel template.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
tunnel	read

Examples

The following example shows the output of the **show tunnel-template test** command for Local PE Tunnel:

```
RP/0/0/CPU0:router# show tunnel-template test
Fri Jan 30 06:22:46.428 UTC

Tunnel template
--------------------------------------------------------
Name:       test (ifhandle: 0x00080030)
MTU:        1464
TTL:        255
TOS:        0
Tunnel ID:  1
Source:     25.25.25.25
Session ID: 0x1D174108 Cookie: 8 bytes [0x24FD3ADAA4485333] being rolled into
    Session ID: 0x15A86E93 Cookie: 8 bytes [0xF486195660CCD522]
Next Session-id/Cookie rollover happens in 1 minute 49 seconds
Transmit:        14213298 pkts  1250770344 bytes
Cookie Mismatch: 0 pkts
MTU Violation:   0 pkts
```

The following example shows the output of the **show tunnel-template test** command for Remote PE Tunnel:

```
RP/0/0/CPU0:router# show tunnel-template test
```

```
Fri Jan 30 06:04:29.800 UTC

Tunnel template
--------------------------------------------------------
Name:       test (ifhandle: 0x00080030)
MTU:        600
TTL:        255
TOS:        0
Tunnel ID:  1
Source:     35.35.35.35    Address Pool: 36.36.36.0/28
Session ID: 0x111F4312 Cookie: 8 bytes [0xB95A806145BE9BE7]
Transmit:        122168722 pkts  10750845295 bytes
Cookie Mismatch: 0 pkts
MTU Violation:   0 pkts
```

Related Commands

Command	Description
tunnel-template, on page 109	Enters tunnel-template configuration submode.

tag-rewrite

To configure VLAN tag rewrite, use the **tag-rewrite** command in Encapsulation MPLS configuration mode. To disable VLAN tag rewrite, use the **no** form of this command.

tag-rewrite ingress vlan *vlan-id*

no tag-rewrite ingress vlan *vlan-id*

Syntax Description

ingress	Configures ingress mode.
vlan	Configures VLAN tagged mode
vlan-id	Specifies the value of the ID of the VLAN.

Command Default

None

Command Modes

Encapsulation MPLS configuration

Command History

Release	Modification
Release 3.7.0	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 **tag-rewrite** command is applicable only to pseudowires with MPLS encapsulation.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure preferred-path tunnel settings:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/0/CPU0:router(config-l2vpn-pwc)# encapsulation mpls
RP/0/0/CPU0:router(config-l2vpn-pwc-encap-mpls)# tag-rewrite vlan 2000
RP/0/0/CPU0:router(config-l2vpn-pwc-encap-mpls)#
```

Related Commands

Command	Description
show l2vpn xconnect, on page 93	Displays brief information on configured cross-connects.

timeout setup (L2TP)

To configure timeout definitions for L2TP session setup, use the **timeout setup** command in L2TP class configuration mode. To return to the default behavior, use the **no** form of this command.

timeout setup *seconds*

no timeout setup *seconds*

Syntax Description

seconds	Time, in seconds, to setup a control channel. Range is 60 to 6000 seconds. Default is 300 seconds.

Command Default

seconds: 300

Command Modes

L2TP class configuration

Command History

Release	Modification
Release 3.7.0	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 timeout value for L2TP session setup of 400 seconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2tp-class cisco
RP/0/0/CPU0:router(config-l2tp-class)# timeout setup 400
```

Related Commands

Command	Description
authentication (L2TP), on page 3	Enables L2TP authentication for a specified L2TP class name.

Command	Description
hello-interval (L2TP), on page 26	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 28	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 30	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 34	Enters L2TP class configuration mode where you can define an L2TP signaling template.
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
receive-window (L2TP), on page 65	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 67	Configures retransmit retry and timeout values.
show l2tp session, on page 77	Displays information about L2TP sessions.
show l2tp tunnel, on page 79	Displays information about L2TP tunnels.

transport mode (L2VPN)

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

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

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

Syntax Description

ethernet	Configures Ethernet port mode.
vlan	Configures VLAN tagged mode.

Command Default

None

Command Modes

L2VPN pseudowire class MPLS encapsulation

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 configure Ethernet transport mode:

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

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

Related Commands

Command	Description
pw-class (L2VPN), on page 57	Enters pseudowire class submode to define a pseudowire class template.

tunnel-template

To enter tunnel-template configuration submode, use the **tunnel-template** command in global configuration mode.

tunnel-template *template name*

no tunnel-template *template-name*

Syntax Description

template-name	Configures a name for the tunnel template.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.5.0	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
tunnel	read, write

Examples

The following example shows how to enter tunnel-template configuration submode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# tunnel-template template_01
```

Related Commands

Command	Description
xconnect group, on page 110	Configures cross-connect groups.

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 3.4.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# xconnect group customer_atlantic
```

Related Commands

Command	Description
show l2vpn xconnect, on page 93	Displays brief information on configured cross-connects.

Virtual Private LAN Services Commands

This module describes the commands used to configure, monitor, and troubleshoot Virtual Private LAN Services (VPLS).

For detailed information about virtual private network concepts, configuration tasks, and examples, refer to the *Virtual Private Configuration Guide*.

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 3.7.0	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 **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/0/0/CPU0:router#configure
RP/0/0/CPU0:router(config)#l2vpn
RP/0/0/CPU0:router(config-l2vpn)#bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)#bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)#mac
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac)#limit
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac-limit)#action flood
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac-limit)#maximum 10
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	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 133	Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 137	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 145	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 175 and the type (VPLS), on page 177 parameters.

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.0	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 **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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# time 120
```

Related Commands

Commands	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then assigns network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.
time (VPLS), on page 175	Configures the maximum aging time.
type (VPLS), on page 177	Configures the type for MAC address aging.

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 3.7.0	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 **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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)#
```

Related Commands

Command	Description
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	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 3.7.0	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 **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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
l2vpn, on page 47	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 3.7.0	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 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/0/0/CPU0:router# clear l2vpn bridge-domain all
```

Related Commands

Command	Description
show l2vpn bridge-domain (VPLS), on page 151	Display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains.

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 3.7.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# flooding disable
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mtu (VPLS), on page 141	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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# flooding unknown-unicast disable
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mtu (VPLS), on page 141	Adjusts the maximum packet size or maximum transmission unit (MTU) size for the bridge domain.

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 3.7.0	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 **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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/9
RP/0/0/CPU0:router(config-l2vpn-bg-bd-ac)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.

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 3.7.0	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.

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.

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 3.7.0	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 **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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# mac
```

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

Related Commands

Command	Description
action (VPLS), on page 115	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 137	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 145	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 3.7.0	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 **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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac)#
```

Related Commands

Command	Description
aging (VPLS), on page 117	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
learning disable (VPLS), on page 131	Overrides the MAC learning configuration of a parent bridge or sets the MAC learning configuration of a bridge.
limit (VPLS), on page 133	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 171	Adds static entries to the MAC address for filtering.
withdraw (VPLS), on page 181	Disables MAC address withdrawal for a specified bridge domain

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 3.7.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac)# limit
```

```
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# maximum 5000
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# action no-flood
```

Related Commands

Command	Description
action (VPLS), on page 115	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
limit (VPLS), on page 133	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 135	Enters L2VPN bridge group bridge domain MAC configuration mode.
notification (VPLS), on page 145	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

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 3.7.0	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.

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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# vfi model
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# mpls static label local 800 remote 500
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
neighbor (VPLS), on page 143	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
pw-class (VFI), on page 149	Configures the pseudowire class template name to use for the pseudowire.
vfi (VPLS), on page 179	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 3.7.0	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.

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).

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example specifies an MTU of 1000 bytes:

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

```
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# mtu 1000
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	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 125	Configures flooding for traffic at the bridge domain level or at the bridge port level.
l2vpn, on page 47	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 3.7.0	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 **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/0/0/CPU0:router# configure
```

```
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# neighbor 10.1.1.2 pw-id 1000
RP/0/0/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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 139	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
pw-class (VFI), on page 149	Configures the pseudowire class template name to use for the pseudowire.
static-mac-address (VPLS), on page 173	Configures the static MAC address to associate a remote MAC address with a pseudowire or any other bridge interface.
vfi (VPLS), on page 179	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 3.7.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac)# limit
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# notification both
```

Related Commands

Command	Description
action (VPLS), on page 115	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 137	Configures the specified action when the number of MAC addresses learned on a bridge is reached.

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

Related Commands

Command	Description
action (VPLS), on page 115	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 137	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 145	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

pw-class (VFI)

To configure the pseudowire class template name to use for the pseudowire, use the **pw-class** command in L2VPN bridge group bridge domain VFI 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 VFI pseudowire configuration

Command History

Release	Modification
Release 3.7.0	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 attach the pseudowire class to the pseudowire:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# pw-class canada
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 139	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 143	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
vfi (VPLS), on page 179	Configures virtual forwarding interface (VFI) parameters.

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 [**bd-name bridge-domain-name**| **brief**| **detail**| **group bridge-domain-group-name**| **interface type interface-path-id**]**neighbor IP-address** [**pw-id value**| **summary**]

Syntax Description

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.
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.
summary	(Optional) Displays the summary information for the bridge domain.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	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 **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

This table describes the significant fields shown in the display.

The following sample output shows information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains:

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

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
```

This table describes the significant fields shown in the display.

Table 9: 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.

The following example shows sample output for a bridge named bd1:

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

Bridge Group/Bridge-Domain Name  ID    State      Num ACs/up     Num PWs/up
-------------------------------- ----- ---------- -------------- --------------
g1/bd1                           0     up         1/1            1/1
```

This table describes the significant fields shown in the display.

Table 10: 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/0/0/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 (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: 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
```

The following sample output shows that when a bridge operates in VPWS mode, the irrelevant information for MAC learning is suppressed:

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

Bridge group: foo_group, bridge-domain: foo_bd, id: 0, state: up, ShgId: 0
  VPWS Mode
  MTU: 1500
  ACs: 1 (0 up), VFIs: 1, PWs: 2 (2 up)
  List of ACs:
    AC: GigabitEthernet0/5/1/4, state is admin down
      Type Ethernet      MTU 1500; XC ID 1; interworking none
    Static MAC addresses:
      Statistics:
        packet totals: receive 0,send 0
        byte totals: receive 0,send 0
  List of VFIs:
    VFI foo_vfi
      PW: neighbor 1.1.1.1, PW ID 1, state is up ( established )
        PW class not set
        Encapsulation MPLS, protocol LDP
        PW type Ethernet, control word enabled, interworking none
```

```
  Sequencing not set
    MPLS         Local                          Remote
    ------------ ------------------------------ ------------------------------
    Label        16001                          16001
    Group ID   unassigned                     unknown
    Interface    siva/vfi                       siva/vfi
    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: 25/06/2007 05:29:42 (2w0d ago)
  Last time status changed: 27/06/2007 06:50:35 (1w5d ago)
Static MAC addresses:
PW: neighbor 1.1.1.1, PW ID 2, state is up ( established )
  PW class not set
  Encapsulation MPLS, protocol LDP
  PW type Ethernet, control word enabled, interworking none
  Sequencing not set
    MPLS         Local                          Remote
    ------------ ------------------------------ ------------------------------
    Label        16002                          16002
    Group ID     unassigned                     unknown
    Interface    siva/vfi                       siva/vfi
    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: 25/06/2007 05:29:42 (2w0d ago)
  Last time status changed: 27/06/2007 06:50:35 (1w5d ago)
Static MAC addresses:
Statistics:
  drops: illegal VLAN 0, illegal length 0
```

This table describes the significant fields shown in the display.

Table 11: 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.
MSTi	ID for the Multiple Spanning Tree.

The following sample output shows filter information about the bridge-domain group named g1:

```
RP/0/0/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 1.1.1.1 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/0/0/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/0/0/CPU0:router# show l2vpn bridge-domain neighbor 1.1.1.1

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 1.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
```

The following sample output shows the summary information for the bridge domain:

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

Number of groups: 1, bridge-domains: 1, Up: 1, Shutdown: 0
Number of ACs: 1 Up: 1, Down: 0
Number of PWs: 1 Up: 1, Down: 0
```

This table describes the significant fields shown in the display.

Table 12: 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.

Related Commands

Command	Description
clear l2vpn bridge-domain (VPLS), on page 123	Clears the MAC addresses and restarts the bridge domains on the router.

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 3.7.0	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.

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/0/0/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/0/0/CPU0:router

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
```

```
================ GSR HW Information ================

------------------------------------------------
           SHG-TX rewrite details
------------------------------------------------
------------------------------------------------
 HW Rewrite 0 Detail :
------------------------------------------------
    Rewrite HW Address  : 0x00060000
    packets 0  bytes 0
 Raw data:
[ 0x04018180 04018190 040181a0 040181b0 ]
[ 0x04018170 00000000 80360000 000bfff4 ]
[ 0x00000000 00000000 00000000 00000000 ]

------------------------------------------------
           SHG-TX encap details
------------------------------------------------
outer_etype:                    0
outer_vlan_id:                  0
gather_profile:                 0
inner_vlan_id:                  0
so_l2_len_adjust:               0
------------------------------------------------
           SHG-TX mgid details
------------------------------------------------
          Base MGIDs for default mgid
base_mgid[0]:              0x0003fffb
base_mgid[1]:              0x0003fffb
base_mgid[2]:              0x0003fffb
base_mgid[3]:              0x0003fffb
base_mgid[4]:              0x0003fffb
base_mgid[5]:              0x0003fffb
base_mgid[6]:              0x0003fffb
base_mgid[7]:              0x0003fffb
         MGID Entries for default mgid
oi[0]:              0
oq[0]:              16384
xc_id[0]:           1
mgid_idx[0]:        0x00000000
next_mgid[0]:       0x00000000
------------------------------------------------
 VMR 0 Details
------------------------------------------------
vmrid: 0x5f002010
Value: 0xc0 0x00 0x1f 0xff 0xff 0xff 0xff 0xff 0xfd
Mask : 0x00 0x00 0x1f 0xff 0xff 0xff 0xff 0xff 0xe0
Result 0x32003000
================================================

  GigabitEthernet0/1/0/0, state: oper up
    Number of MAC: 32770
    Sent(Packets/Bytes): 749/22989834
    Received(Packets/Bytes): 5732104/447104112

================ GSR HW Information ================

------------------------------------------------
           BP-TX-AC rewrite details
------------------------------------------------

 BP is local


------------------------------------------------
 BP L2 Uidb Details
------------------------------------------------
l2fwd_enabled:                  true
plim_enabled:                   true
l2fwd_type:                     4
l2_ac_type:                     0
xconn_id:                       0
```

```
bridge_id:                      0
shg id:                         0
unicast flooding enabled:       0
multicast flooding enabled:     0
broadcast flooding enabled:     0
mac learning enabled:           0
Is AC Port mode?:           0
-------------------------------------------------
 HW Rewrite 0 Detail :
-------------------------------------------------
    Rewrite HW Address  : 0x59eff314
    packets 0  bytes 0
    HFA Bits 0x0 gp 0 mtu 1580  (REW)
    OI 0x3fffc OutputQ 0 Output-port 0x36 local_outputq 0x0
 Raw data:
[ 0x00000000 0036062c 0003fffc 00000000 ]
[ 0x00000000 00000000 0d103600 00000010 ]
[ 0x00000000 00000000 00000000 00000000 ]

-------------------------------------------------
 BP OI/OQ Details
-------------------------------------------------
oi[0]:          0x00000000        oq[0]             16384
oi[1]:          0x00000000        oq[1]             65535
oi[2]:          0x00000000        oq[2]             65535
oi[3]:          0x00000000        oq[3]             65535
oi[4]:          0x00000000        oq[4]             65535
oi[5]:          0x00000000        oq[5]             65535
oi[6]:          0x00000000        oq[6]             65535
oi[7]:          0x00000000        oq[7]             65535
-------------------------------------------------
 Sram table entry details
-------------------------------------------------
sram_data: 0xa000400c
=================================================

  Nbor 1.1.1.1 pw-id 1
    Number of MAC: 32766
    Sent(Packets/Bytes): 0/0
    Received(Packets/Bytes): 5731250/447037500

================ GSR HW Information ================

-------------------------------------------------
           BP-TX-AC rewrite details
-------------------------------------------------
-------------------------------------------------
 BP OI/OQ Details
-------------------------------------------------
oi[0]:          0x00000000        oq[0]             65535
oi[1]:          0x00000000        oq[1]             65535
oi[2]:          0x00000000        oq[2]             65535
oi[3]:          0x00000000        oq[3]             65535
oi[4]:          0x00000000        oq[4]             65535
oi[5]:          0x00000000        oq[5]             65535
oi[6]:          0x00000000        oq[6]             65535
oi[7]:          0x00000000        oq[7]             65535
-------------------------------------------------
 BP Encap Info
-------------------------------------------------
mac_length:   0
mac_string:
egress_slot:  2
num_tags:     1
 tags:        {16001, }
if_handle:    0x03000500
=================================================
```

The following sample output shows the bridge-domain information for the specified location:

```
RP/0/0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 location 0/1/CPU0

Bridge-Domain Name               ID     Ports addr   Flooding Learning State
```

```
------------------------------- ------ ----- ------ -------- -------- ---------
g1:bd1                          0      2     65536  Enabled  Enabled  UP
```

This table describes the significant fields shown in the display.

Table 13: 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.

Related Commands

Command	Description
clear l2vpn bridge-domain (VPLS), on page 123	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/0/0/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/0/0/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/0/0/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/0/0/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/0/0/CPU0:router# show l2vpn forwarding bridge-domain mac-address neighbor 1.1.1.1 pw-id
 1 location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
------------------------------------------------------------------------------
0000.0003.0101 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0102 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0103 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0104 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0105 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0106 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0107 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0108 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0109 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010a dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010b dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010c dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010d dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010e dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.010f dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0110 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0111 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0112 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0113 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0114 dynamic 1.1.1.1, 1                  0/1/CPU0   0d 0h 0m 30s
0000.0003.0115 dynamic 1.1.1.1, 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/0/0/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
```

Related Commands

Command	Description
show l2vpn forwarding bridge-domain (VPLS), on page 158	Displays information on the bridge that is used by the forwarding layer.

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 3.7.0	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.

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	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 3.7.0	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 disable VFI:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi)# shutdown
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 139	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 143	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).

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 3.7.0	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 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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac)# static-address 1.1.1 drop
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	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 3.7.0	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 associate a remote MAC address with a pseudowire:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# vfi model
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/0/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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/1/0/0
RP/0/0/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/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# neighbor 10.1.1.2 pw-id 2000
RP/0/0/CPU0:router(config-l2vpn-bg-bd-pw)# static-mac-address 2.2.2
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 139	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 143	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
vfi (VPLS), on page 179	Configures virtual forwarding interface (VFI) parameters.

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 3.7.0	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.

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

```
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# time 600
```

Related Commands

Command	Description
aging (VPLS), on page 117	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.
type (VPLS), on page 177	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 3.7.0	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.

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

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

Related Commands

Command	Description
aging (VPLS), on page 117	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.
time (VPLS), on page 175	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 3.7.0	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 **vfi** command to enter L2VPN bridge group bridge domain VFI configuration mode.

You cannot configure a pseudowire directly under a bridge domain. Therefore, a psuedowire must be configured under a VFI, which is configured under a bridge domain.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to create a VFI:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 139	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 143	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).

withdraw (VPLS)

To enable MAC address withdrawal for a specified bridge domain, use the **withdraw** command in L2VPN bridge group bridge domain MAC configuration mode. To disable this feature, use the **no** form of this command

withdraw { **disable**}

no withdraw { **disable** }

Syntax Description

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 3.7.0	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 enable disable MAC withdrawal:

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

The following example shows how to disable sending MAC withdrawal messages to access pseudowires:

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

```
RP/0/0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/0/CPU0:router(config-l2vpn-bg-bd-mac)# withdraw access-pw disable
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 119	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 121	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 47	Enters L2VPN configuration mode.
mac (VPLS), on page 135	Enters L2VPN bridge group bridge domain MAC configuration mode.

INDEX

P

R

S

T

V

W

X