



# Cisco IOS XR Virtual Private Network Command Reference for the Cisco CRS Router, Release 6.1.x

**First Published: 2016-11-01** 

# **Americas Headquarters**

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

Fax: 408 527-0883

# **Full Cisco Trademarks with Software License**

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016 Cisco Systems, Inc. All rights reserved.



# CONTENTS

### Full Cisco Trademarks with Software License ii

### PREFACE

### Preface ix

Changes to This Document ix

Communications, Services, and Additional Information ix

#### CHAPTER 1

### **Ethernet Interfaces Commands** 1

encapsulation dot1ad dot1q 2

encapsulation dot1q 4

encapsulation dot1q second-dot1q 5

12transport (Ethernet) 6

rewrite ingress tag 7

### CHAPTER 2

### **Virtual Private Network Commands** 9

authentication (L2TP) 11

backup disable (L2VPN) 13

clear l2tp counters control session 15

clear 12tp counters control tunnel **16** 

clear 12tp tunnel 17

clear l2vpn collaborators 18

clear l2vpn counters l2tp 19

clear 12vpn counters bridge mac-withdrawal 20

clear 12vpn forwarding counters 21

clear 12vpn forwarding mac-address-table 22

clear 12vpn forwarding message counters 24

clear 12vpn forwarding table 25

```
digest (L2TP) 26
hello-interval (L2TP) 28
hidden (L2TP) 30
hostname (L2TP) 32
interface (p2p) 34
12tp-class 36
12transport 37
12transport 12protocol 39
12transport propagate 41
12transport service-policy
12vpn 44
load-balancing flow-label 45
logging (l2vpn) 47
logging nsr 48
monitor-session (l2vpn) 49
mpls static label (L2VPN) 50
neighbor (L2VPN) 52
nsr (L2VPN) 54
password (L2TP) 55
pw-class (L2VPN) 57
pw-class encapsulation 12tpv3
pw-class encapsulation mpls 60
pw-ether 62
pw-grouping 64
p2p 65
receive-window (L2TP) 66
retransmit (L2TP) 68
rollover (L3VPN) 70
show generic-interface-list
show 12tp class 73
show 12tp counters forwarding session 75
show 12tp session 77
show 12tp tunnel 79
show 12vpn 81
```

```
show 12vpn generic-interface-list 99
     show 12vpn index 101
     show 12vpn nsr
     show l2vpn process fsm 105
     show 12vpn provision queue 107
     show l2vpn pw-class 109
     show 12vpn pwhe 111
     show l2vpn resource 113
     show l2vpn trace 114
     show l2vpn xconnect 116
     show tunnel-template 126
                    128
     storm-control
     tag-impose 131
     tag-rewrite 132
     timeout setup (L2TP) 133
     transport mode (L2VPN) 135
     transport mode vlan passthrough
     tunnel-template 137
     xconnect group 138
Virtual Private LAN Services Commands 139
     action (VPLS) 140
     aging (VPLS) 142
     bridge-domain (VPLS) 144
     bridge group (VPLS) 145
     clear 12vpn bridge-domain (VPLS) 146
     flooding disable 147
     interface (VPLS) 149
     learning disable (VPLS) 151
```

CHAPTER 3

show 12vpn atom-db 82 show 12vpn collaborators 85 show 12vpn database 87 show 12vpn forwarding 90

show 12vpn forwarding 12tp 98

```
limit (VPLS) 153
mac (VPLS) 155
maximum (VPLS) 157
mpls static label (VPLS) 159
mtu (VPLS) 161
neighbor (VPLS) 163
notification (VPLS) 165
port-down flush disable (VPLS) 167
pw-class (VFI) 169
show l2vpn bridge-domain (VPLS) 171
show l2vpn forwarding bridge-domain (VPLS) 180
show 12vpn forwarding bridge-domain mac-address (VPLS) 196
shutdown (Bridge Domain) 207
shutdown (VFI) 208
static-address (VPLS) 210
static-mac-address (VPLS) 212
time (VPLS) 214
type (VPLS) 216
vfi (VPLS) 218
withdraw (VPLS) 220
```

# CHAPTER 4 Generic Routing Encapsulation Commands 223

```
interface tunnel-ip 224
keepalive 225
tunnel destination 226
tunnel dfbit 227
tunnel mode 228
tunnel source 229
tunnel tos 231
tunnel ttl 232
```



# **Preface**

The preface contains these sections:

- Changes to This Document, on page ix
- Communications, Services, and Additional Information, on page ix

# **Changes to This Document**

The following table lists the technical changes made to this document since it was first published.

Date	Change Summary
November 2016	Initial release of this document.

# **Communications, Services, and Additional Information**

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

# **Cisco Bug Search Tool**

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

**Communications, Services, and Additional Information** 



# **Ethernet Interfaces Commands**

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



Note

This module does not include the commands for Management Ethernet interfaces and Ethernet OAM. To configure a Management Ethernet interface for routing or modify the configuration of a Management Ethernet interface or to configure Ethernet OAM, use the commands described in the *Interface and Hardware Component Configuration Guide for Cisco CRS Routers* 

Refer to the *Interface and Hardware Component Command Reference for Cisco CRS Routers* for more information on the Ethernet Interfaces and Ethernet OAM commands.

- encapsulation dot1ad dot1q, on page 2
- encapsulation dot1q, on page 4
- encapsulation dot1q second-dot1q, on page 5
- 12transport (Ethernet), on page 6
- rewrite ingress tag, on page 7

# encapsulation dot1ad dot1q

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

encapsulation dot1ad vlan-id dot1q {vlan-id | any} no encapsulation dot1ad vlan-id dot1q {vlan-id | any}

### **Syntax Description**

dot1ad Indicates that the IEEE 802.1ad provider bridges encapsulation type is used for the outer tag.

**dot1q** Indicates that the IEEE 802.1q standard encapsulation type is used for the inner tag.

vlan-id VLAN ID, integer in the range 1 to 4094.

any Matches any VLAN ID.

### **Command Default**

No matching criteria are defined.

### **Command Modes**

Subinterface configuration

### **Command History**

Release	Modification
Release 5.1.1	This command was introduced.

# **Usage Guidelines**

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

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

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

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

- MSTP uses the IEEE 802.1ad MAC STP address instead of the STP MAC address.
- Certain QoS functions may use the Drop Eligibility (DE) bit of the IEEE 802.1ad tag.

### **Examples**

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

RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1ad 100 dot1q 20

Command	Description
encapsulation dot1q, on page 4	Defines the matching criteria to map 802.10 frames ingress on an interface to the appropriate service instance.

# encapsulation dot1q

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

encapsulation dot1q vlan-id no encapsulation

### **Syntax Description**

**vlan-id** VLAN ID, integer in the range 1 to 4094.

#### **Command Default**

No matching criteria are defined.

#### **Command Modes**

Subinterface configuration

### **Command History**

Release	Modification
Release 5.1.1	This command was introduced.

#### **Usage Guidelines**

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

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

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

### **Examples**

The following example shows how to map 802.1Q frames ingress on an 12transport subinterface:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/3.10 12transport
RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 10

Command	Description
encapsulation dot1ad dot1q, on page 2	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 5	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.

# encapsulation dot1q second-dot1q

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

encapsulation dot1q {any | vlan-id | second-dot1q {any | vlan-id | } no encapsulation dot1q {any | vlan-id | second-dot1q {any | vlan-id | }

### **Syntax Description**

vlan-id	VLAN ID, integer in the range 1 to 4094.
	A maximum of nine ranges or individual values may be specified. The values must not overlap.
second-dot1q	(Optional) Specifies IEEE 802.1Q VLAN tagged packets.
any	Any second tag in the range 1 to 4094.

#### **Command Default**

No matching criteria are defined.

### **Command Modes**

Subinterface configuration

#### **Command History**

Release	Modification
Release 5.1.1	This command was introduced.

### **Usage Guidelines**

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

The criteria for this command are: the outer tag must be unique and the inner tag may be a single VLAN.

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

Only one encapsulation command must be configured per service instance.

#### **Examples**

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

RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q second-dot1q 20

Command	Description
encapsulation dot1ad dot1q, on page 2	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q, on page 4	Defines the matching criteria to map 802.10 frames ingress on an interface to the appropriate service instance.

# **I2transport (Ethernet)**

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

# 12transport no 12transport

This command has no keywords or arguments.

### **Command Default**

None

### **Command Modes**

Interface or Subinterface configuration

### **Command History**

Release	Modification
Release 5.1.1	This command was introduced.

### **Usage Guidelines**

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

### Task ID

Task ID	Operations
l2vpn	read, write

# **Examples**

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

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/3.10 12transport
RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 10

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

# rewrite ingress tag

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

rewrite ingress tag {push {dot1q  $vlan-id \mid dot1q \ vlan-id \mid second-dot1q \ vlan-id \mid dot1ad \ vlan-id \mid dot1ad \ vlan-id \mid dot1ad \ vlan-id \mid dot1ad \ vlan-id \mid 2 \mid translate {1to1 {dot1q \ vlan-id \mid dot1ad \ vlan-id} \mid 2-to-1 \ dot1q \ vlan-id \mid dot1ad \ vlan-id \mid 1-to-2 \ {dot1q \ vlan-id \mid second-dot1q \ vlan-id \mid dot1ad \ vlan-id \ dot1ad \ vlan-id \ } [symmetric]$ no rewrite tag [symmetric]

# **Syntax Description**

vlan-id	VLAN ID, integer in the range 1 to 4094.
push dot1q vlan-id	Pushes one 802.1Q tag with <i>vlan-id</i> .
push dot1q vlan-id second-dot1q vlan-id	Pushes a pair of 802.1Q tags in the order first, second.
pop {1   2}	One or two tags are removed from the packet. This command can be combined with a push (pop N and subsequent push <i>vlan-id</i> ).
translate 1-to-1 dot1q vlan-id	Replaces the incoming tag (defined in the encapsulation command) into a different 802.1Q tag at the ingress service instance.
translate 2-to-1 dot1q vlan-id	Replaces a pair of tags defined in the <b>encapsulation</b> command by vlan-id.
translate 1-to-2 dot1q vlan-id second-dot1q vlan-id	Replaces the incoming tag defined by the encapsulation command by a pair of 802.1Q tags.
translate 2-to-2 dot1q vlan-id second-dot1q vlan-id	Replaces the pair of tags defined by the encapsulation command by a pair of VLANs defined by this rewrite.
symmetric	(Optional) A rewrite operation is applied on both ingress and egress. The operation on egress is the inverse operation as ingress.

### **Command Default**

The frame is left intact on ingress.

### **Command Modes**

Subinterface configuration

# **Command History**

Release	Modification
Release 5.1.1	This command was introduced.

# **Usage Guidelines**

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

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

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

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

### **Examples**

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

RP/0/RP0/CPU0:router(config-subif)# rewrite ingress push dot1q 200

Command	Description
encapsulation dot1ad dot1q, on page 2	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q, on page 4	Defines the matching criteria to map 802.10 frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 5	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.



# **Virtual Private Network Commands**

For detailed information about virtual private network concepts, configuration tasks, and examples, refer to the *Virtual Private Network Configuration Guide for Cisco CRS Routers* 

- authentication (L2TP), on page 11
- backup disable (L2VPN), on page 13
- clear 12tp counters control session, on page 15
- clear 12tp counters control tunnel, on page 16
- clear 12tp tunnel, on page 17
- clear 12vpn collaborators, on page 18
- clear 12vpn counters 12tp, on page 19
- clear 12vpn counters bridge mac-withdrawal, on page 20
- clear 12vpn forwarding counters, on page 21
- clear 12vpn forwarding mac-address-table, on page 22
- clear 12vpn forwarding message counters, on page 24
- clear 12vpn forwarding table, on page 25
- digest (L2TP), on page 26
- hello-interval (L2TP), on page 28
- hidden (L2TP), on page 30
- hostname (L2TP), on page 32
- interface (p2p), on page 34
- 12tp-class, on page 36
- 12transport, on page 37
- 12transport 12protocol, on page 39
- 12transport propagate, on page 41
- 12transport service-policy, on page 43
- 12vpn, on page 44
- load-balancing flow-label, on page 45
- logging (l2vpn), on page 47
- logging nsr, on page 48
- monitor-session (12vpn), on page 49
- mpls static label (L2VPN), on page 50
- neighbor (L2VPN), on page 52
- nsr (L2VPN), on page 54
- password (L2TP), on page 55

- pw-class (L2VPN), on page 57
- pw-class encapsulation 12tpv3, on page 58
- pw-class encapsulation mpls, on page 60
- pw-ether, on page 62
- pw-grouping, on page 64
- p2p, on page 65
- receive-window (L2TP), on page 66
- retransmit (L2TP), on page 68
- rollover (L3VPN), on page 70
- show generic-interface-list, on page 71
- show 12tp class, on page 73
- show 12tp counters forwarding session, on page 75
- show 12tp session, on page 77
- show 12tp tunnel, on page 79
- show l2vpn, on page 81
- show 12vpn atom-db, on page 82
- show 12vpn collaborators, on page 85
- show 12vpn database, on page 87
- show l2vpn forwarding, on page 90
- show 12vpn forwarding 12tp, on page 98
- show l2vpn generic-interface-list, on page 99
- show 12vpn index, on page 101
- show 12vpn nsr, on page 103
- show 12vpn process fsm, on page 105
- show 12vpn provision queue, on page 107
- show 12vpn pw-class, on page 109
- show 12vpn pwhe, on page 111
- show 12vpn resource, on page 113
- show 12vpn trace, on page 114
- show 12vpn xconnect, on page 116
- show tunnel-template, on page 126
- storm-control, on page 128
- tag-impose, on page 131
- tag-rewrite, on page 132
- timeout setup (L2TP), on page 133
- transport mode (L2VPN), on page 135
- transport mode vlan passthrough, on page 136
- tunnel-template, on page 137
- xconnect group, on page 138

# 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 3.9.0	This command was introduced.

# **Usage Guidelines**

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



#### Note

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class cisco
RP/0/RP0/CPU0:router(config-12tp-class)# authentication
```

Command	Description
hello-interval (L2TP), on page 28	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 30	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 32	Defines the name used in the L2TP hostname AVP.

Command	Description
l2tp-class, on page 36	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 66	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 68	Configures retransmit retry and timeout values.

# backup disable (L2VPN)

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

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

### **Syntax Description**

<b>delay</b> value		
	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.
Release 5.2.1	This command was introduced.

### **Usage Guidelines**

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

#### Task ID

ID	
1	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# pw-class class1
RP/0/RP0/CPU0:router(config-12vpn-pwc)# backup disable delay 50
RP/0/RP0/CPU0:router(config-12vpn-pwc)# exit
RP/0/RP0/CPU0:router(config-12vpn)# xconnect group A
RP/0/RP0/CPU0:router(config-12vpn-xc)# p2p rtrx
RP/0/RP0/CPU0:router(config-12vpn-xc-p2p)# neighbor 10.1.1.1 pw-id 2
```

```
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p-pw)# pw-class class1
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)#
```

Command	Description
l2vpn, on page 44	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 52	Configures a pseudowire for a cross-connect.
p2p, on page 65	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 138	Configures cross-connect groups.

# clear I2tp counters control session

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

clear 12tp 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.
Release 5.2.1	This command was introduced.

# **Usage Guidelines**

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

### Task ID

Task ID	Operations
12vpn	read, write

# **Examples**

The following example shows how to clear all L2TP state machine transition counters:

RP/0/RP0/CPU0:router(config-12vpn-xc-p2p-pw-backup)## clear 12tp counters control session
fsm state transition

Command	Description
clear I2tp counters control tunnel, on page 16	Clears L2TP control counters for a tunnel.
clear I2vpn counters I2tp, on page 19	Clears L2VPN statistical information, such as, packets dropped.

# clear I2tp counters control tunnel

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

clear 12tp 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 3.9.0	This command was introduced.

### **Usage Guidelines**

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

### Task ID

Task ID	Operations
l2vpn	read, write

### **Examples**

The following example shows how to clear all L2TP control tunnel counters:

RP/0/RP0/CPU0:router# clear 12tp counters control tunnel all

Command	Description
clear l2tp counters control session, on page 15	Clears L2TP control counters for a session.
clear I2vpn counters I2tp, on page 19	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 12tp tunnel {all | id tunnel id | 12tp-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.
12tp-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 3.9.0	This command was introduced.

# **Usage Guidelines**

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

### Task ID

Task ID	Operations
12vpn	read, write

# **Examples**

The following example shows how to clear all L2TP tunnels:

RP/0/RP0/CPU0:router# clear 12tp tunnel all

Command	Description
clear l2tp counters control session, on page 15	Clears L2TP control counters for a session.
clear l2tp counters control tunnel, on page 16	Clears L2TP control counters for a tunnel.

# clear I2vpn collaborators

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

# clear 12vpn 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
12vpn	read, write

# **Examples**

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

RP/0/RP0/CPU0:router# clear 12vpn collaborators

Command	Description
show I2vpn collaborators, on page 85	Displays information about the state of the interprocess communications connections between I2vpn_mgr and other processes.

# clear I2vpn counters I2tp

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

clear 12vpn counters 12tp [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 3.9.0	This command was introduced.

# **Usage Guidelines**

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

# Task ID

Task ID	Operations
12vpn	read, write

# **Examples**

The following example shows how to clear all L2TP counters:

RP/0/RP0/CPU0:router# clear 12vpn counters 12tp

Command	Description
show I2vpn collaborators, on page 85	Displays information about the state of the interprocess communications connections between l2vpn_mgr and other processes.

# clear I2vpn 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 12vpn counters bridge mac-withdrawal {all|group group-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.
<b>neighbor</b> <i>ip-address</i>	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 3.9.0	This command was introduced.

### **Usage Guidelines**

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

# Task ID

Task ID	Operations
l2vpn	read, write

### **Examples**

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

RP/0/RP0/CPU0:router# clear 12vpn counters bridge mac-withdrawal all

# clear I2vpn forwarding counters

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

clear 12vpn forwarding counters

**Syntax Description** 

This command has no arguments or keywords.

**Command Default** 

Vone

**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
12vpn	read, write

### **Examples**

The following example shows how to clear L2VPN forwarding counters:

RP/0/RP0/CPU0:router# clear 12vpn forwarding counters

Command	Description
show I2vpn forwarding, on page 90	Displays forwarding information from the layer2_fib manager on the line card.

# clear I2vpn 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 | 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 <b>show interfaces</b> 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 <i>node-id</i> argument is entered in the <i>rack/slot/module</i> 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
12vpn	read, write, execute

### **Examples**

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

 ${\tt RP/0/RP0/CPU0:} router {\tt\# clear 12vpn forwarding mac-address location 1/1/1}$ 

Command	Description
show I2vpn forwarding, on page 90	Displays forwarding information from the layer2_fib manager on the line card.

# clear I2vpn forwarding message counters

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

clear 12vpn 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	

Λ-			11:-4-	
L0	mm	ana	Histo	rv

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
12vpn	read, write

### **Examples**

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

RP/0/RP0/CPU0:router# clear 12vpn forwarding message counters location 0/6/CPU0

Command	Description
show I2vpn forwarding, on page 90	Displays forwarding information from the layer2_fib manager on the line card.

# clear I2vpn forwarding table

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

clear 12vpn forwarding table location node-id

Syntax Description	locatio node-io		lears L2VPN forwarding ta	bles for the specified location.	-
Command Default	None				
Command Modes	EXEC				
Command History	Releas	e Mod	lification		
	Releas	e 3.4.0 This	s command was introduced.		
Usage Guidelines		the user grou			up that includes appropriate task ontact your AAA administrator
Task ID	Task ID	Operations	-		
	12vpn	read, write	-		

# **Examples**

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

RP/0/RP0/CPU0:router# clear 12vpn forwarding table location 1/2/3/5

Related Commands	Command	Description	
	show I2vpn forwarding, on page 90	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 \mid SHA1\} \mid secret \{0 \mid 7word\}\}\$  no digest {check disable | hash  $\{MD5 \mid SHA1\} \mid secret \{0 \mid 7word\}\}\$ 

### **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 3.9.0	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 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
12vpn	read, write

# **Examples**

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

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class cisco

```
RP/0/RP0/CPU0:router(config-12tp-class)# digest check disable
RP/0/RP0/CPU0:router(config-12tp-class)# digest secret cisco hash md5
```

Command	Description
authentication (L2TP), on page 11	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 28	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 30	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 32	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 36	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 66	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 68	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 (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 3.9.0	This command was introduced.

#### **Usage Guidelines**

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

#### Task ID

Task ID	Operations
12vpn	read, write

# **Examples**

The following example shows how to configure the hello-interval value for L2TP to 22 seconds:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class cisco
RP/0/RP0/CPU0:router(config-12tp-class)# hello-interval 22

Command	Description
authentication (L2TP), on page 11	Enables L2TP authentication for a specified L2TP class name.
hidden (L2TP), on page 30	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 32	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 36	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.

Command	Description
receive-window (L2TP), on page 66	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 68	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 3.9.0	This command was introduced.

# **Usage Guidelines**

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

# Task ID

Task ID	Operations
l2vpn	read, write

# **Examples**

The following example shows how to enable hidden AVPs:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class cisco
RP/0/RP0/CPU0:router(config-12tp-class)# hidden

Command	Description
authentication (L2TP), on page 11	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 28	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hostname (L2TP), on page 32	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 36	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 66	Configures the receive window size for the L2TP server.

Command	Description
retransmit (L2TP), on page 68	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 3.9.0	This command was introduced.

# **Usage Guidelines**

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

# Task ID

Task ID	Operations
l2vpn	read, write

#### **Examples**

The following example shows how to configure a hostname using the word "cisco":

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class cisco
RP/0/RP0/CPU0:router(config-12tp-class)# hostname cisco

Command	Description
authentication (L2TP), on page 11	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 28	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 30	Enables hidden attribute-value pairs (AVPs).
l2tp-class, on page 36	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.

Command	Description
receive-window (L2TP), on page 66	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 68	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 [PW-Ether | PW-IW] no interface type interface-path-id [PW-Ether | PW-IW]

# **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 <b>show interfaces</b> 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 (?) o help function.	
PW-Ether	(Optional) Configures an Ethernet Interface.	
PW-IW	(Optional) Configures an IP Interworking Interface.	

# **Command Default**

None

#### **Command Modes**

p2p configuration submode

#### **Command History**

Release	Modification
Release 3.4.0	This command was introduced.
Release 4.2.1	The following keywords were added:
	• PW-Ether
	• PW-IW

# **Usage Guidelines**

To use this command, you must be in a user group associated with a task 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn

RP/0/RP0/CPU0:router(config-l2vpn)# xconnect group gr1
RP/0/RP0/CPU0:router(config-l2vpn-xc)# p2p p001
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p)# interface TenGigE 1/1/1/1

Command	Description
p2p, on page 65	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 3.9.0	This command was introduced.

# **Usage Guidelines**

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



Note

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

# Task ID

Task ID	Operations
12vpn	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class cisco
RP/0/RP0/CPU0:router(config-12tp-class)#

# **I2transport**

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.

# 12transport no 12transport

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
12vpn	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/RP0/CPU0:router(config-if)# 12transport
```

#### **Ethernet VLAN Mode:**

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0.900 12transport
RP/0/RP0/CPU0:router(config-if)# encapsulation dot1q 100do1q vlan 999

#### Ethernet VLAN Mode (QinQ):

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0.900 12transport
RP/0/RP0/CPU0:router(config-if)# encapsulation dot1q 20 second-dot1q 10vlan 999 888

# **Ethernet VLAN Mode (QinAny)**:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0.900 12transport
RP/0/RP0/CPU0:router(config-if)# encapsulation dot1q 30 second-dot1q do1q vlan 999 any

Command	Description
show I2vpn forwarding, on page 90	Displays forwarding information from the layer2_fib manager on the line card.

# **I2transport I2protocol**

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.

12transport 12protocol {cdp | pvst | stp | vtp} {drop | experimental | bits | tunnel | experimental | bits} no | 12transport | 12protocol | {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 3.9.0	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.

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
12vpn	read, write
atm	read, write

# **Examples**

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

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/RP0/CPU0:router(config-if)# 12transport 12protocol cpsv reverse-tunnelstp drop

Command	Description
show I2vpn forwarding, on page 90	Displays forwarding information from the layer2_fib manager on the line card.

# **I2transport propagate**

To propagate Layer 2 transport events, use the **12transport propagate** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

12transport propagate remote-status no 12transport propagate remote-status

# **Syntax Description**

remote-status Propagates remote link status changes.

#### **Command Default**

None

#### **Command Modes**

Interface configuration

# **Command History**

Release	Modification
Release 3.6.0	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 *Interface and Hardware Component Configuration Guide for Cisco CRS Routers* 



# Note

This command is supported on the following Cisco CRS Router SPA cards:

- Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter, Version 2
- Cisco 2-port, 5-port, 8-port, and 10-port Gigabit Ethernet Shared Port Adapters
- Cisco 2-, 5-, 8-, and 10-Port Gigabit Ethernet Shared Port Adapters, Version 2
- Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter

Any port on 6-10GE-WLO-FLEX (irrespective of SPA or fixed) does not support the **l2transport propagate** command.

For more information about the Ethernet remote port shutdown feature, see MPLS Configuration Guide for the Cisco CRS Routers.

# Task ID

Task Operations ID

12vpn read, write

# **Examples**

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

RP/0/RP0/CPU0:router# configure

RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0

RP/0/RP0/CPU0:router(config-if)# 12transport propagate remote remote-status

Command	Description
show I2vpn forwarding, on page 90	Displays forwarding information from the layer2_fib manager on the line card.

# **I2transport 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 3.9.0	This command was introduced.

# **Usage Guidelines**

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

#### Task ID

Task ID	Operations
l2vpn	read, write
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)# 12transport service-policy input sp\_0001

Command	Description
show I2vpn forwarding, on page 90	Displays forwarding information from the layer2_fib manager on the line card.

# **I2vpn**

To enter L2VPN configuration mode, use the **12vpn** 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)#

Command	Description
show I2vpn forwarding, on page 90	Displays forwarding information from the layer2_fib manager on the line card.

# load-balancing flow-label

To balance the load based on flow-labels, use the **load-balancing flow label** command in the l2vpn pseudowire class mpls configuration submode or l2vpn bridge group bridge-domain vfi autodiscovery bgp or ldp signaling submodes. To undo flow-label based load-balancing, use the **no** form of this command.

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

#### **Syntax Description**

both	Inserts or discards flow labels on transmit or receive.
code	Specifies the flow label TLV (type-length-value) code. The code value is 17.
receive	Discards flow label on receive.
transmit	Inserts flow label on transmit.
static	Sets flow label parameters statically.

#### **Command Default**

None

#### **Command Modes**

L2vpn pseudowire class mpls configuration submode

L2vpn bridge group bridge-domain vfi autodiscovery bgp signaling submode

L2vpn bridge group bridge-domain vfi autodiscovery ldp signaling submode

# **Command History**

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.2	The <b>code</b> keyword was introduced.

#### **Usage Guidelines**

To use this command, you must be in a user group associated with a task 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 the draft-ietf-pwe3-fat-pw document, the flow label sub-TLV identifier for the Flow Aware Transport Pseudowire (FAT PW) was 0x11. This value has been changed to 0x17, which is also the sub-TLV identifier assigned by the Internet Assigned Numbers Authority (IANA).

Use the **load-balancing flow label code** command to toggle between the sub-TLV identifiers—0x11 and 0x17. If there is a mismatch between two endpoints in the load-balancing flow label code, then the PWs will have a mismatched TLV value resulting in a load balancing failure.

The no form of the load-balancing flow label code command uses the flow label sub-TLV identifier 0x11.

#### Task ID

Task ID	Operation
l2vpn	read, write

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

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config) #12vpn
RP/0/RP0/CPU0:router(config-12vpn) #pw-class p1
RP/0/RP0/CPU0:router(config-12vpn-pwc) #encapsulation
RP/0/RP0/CPU0:router(config-12vpn-pwc) #encapsulation mpls
RP/0/RP0/CPU0:router(config-12vpn-pwc-mpls) #load-balancing
RP/0/RP0/CPU0:router(config-12vpn-pwc-mpls) #load-balancing flow-label
RP/0/RP0/CPU0:router(config-12vpn-pwc-mpls) #load-balancing flow-label both
RP/0/RP0/CPU0:router(config-12vpn-pwc-mpls) #load-balancing flow-label both
```

Command	Description
pw-class encapsulation mpls, on page 60	Configures MPLS pseudowire encapsulation.

# logging (I2vpn)

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
12vpn	read, write

#### **Examples**

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

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# logging pseudowire status

Command	Description
l2vpn, on page 44	Enters L2VPN configuration mode.

# logging nsr

To enable non-stop routing logging, use the **logging nsr** command in L2VPN configuration submode. To return to the default behavior, use the **no** form of this command.

logging nsr no logging nsr

# **Syntax Description**

This command has no keywords or arguments.

#### **Command Default**

None

#### **Command Modes**

L2VPN configuration submode

# **Command History**

Release	Modification
Release 4.3.0	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
12vpn	read, write

# **Examples**

The following example shows how to enable non-stop routing logging:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# logging nsr

Command	Description
l2vpn, on page 44	Enters L2VPN configuration mode.

# monitor-session (I2vpn)

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

monitor-session session-name no monitor-session session-name

#### **Syntax Description**

session-name Name of the monitor session to configure.

#### **Command Default**

No default behavior or values

#### **Command Modes**

Point-to-point cross connect configuration

#### **Command History**

<b>D</b> I	B
Release	Modification
HEIGASE	www.iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii

Release 4.0.0 This command was introduced.

# **Usage Guidelines**

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

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

#### Task ID

Task ID	Operations
l2vpn	
	write

# **Examples**

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

```
RP/0/RSP0/CPU0:router(config) # 12vpn
RP/0/RSP0/CPU0:router(config-l2vpn) # xconnect group g1
RP/0/RSP0/CPU0:router(config-l2vpn-xc) # p2p xcon1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p) # monitor-session mon1
```

#### **Related Commands**

**Command** Description

See the **monitor session** command in the *Interface and Hardware Component Command Reference for Cisco CRS Routers*.

# 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
12vpn	read, write

#### **Examples**

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

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn xconnect group 12vpn
RP/0/RP0/CPU0:router(config-12vpn-xc)# p2p rtrA\_to\_rtrB
RP/0/RP0/CPU0:router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-12vpn-xc-p2p-pw)# mp1s static label local 800 remote 500

Command	Description
I2vpn, on page 44	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 52	Configures a pseudowire for a cross-connect.
p2p, on page 65	Enters p2p configuration submode to configure point-to-point cross-connects.

Command	Description
xconnect group, on page 138	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.

#### **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.
tag-impose	Optional Specifies a tag during a VLAN ID configuration.

# **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 <b>vccv disable</b> keyword was added.
Release 3.7.0	These keywords were removed:
	<ul><li>control-word</li><li>pw-static-label local</li><li>remote</li><li>vccv</li><li>transport-mode</li></ul>

Release 4.2.1 The keyword **tag-impose** was introduced.

# **Usage Guidelines**

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

A cross-connect may have two segments:

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



Note

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

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

# Task ID Task Operations ID 12vpn read, write

#### **Examples**

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn xconnect group 12vpn
RP/0/RP0/CPU0:router(config-12vpn-xc)# p2p rtrA_to_rtrB
RP/0/RP0/CPU0:router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000 pw-class class12
RP/0/RP0/CPU0:router(config-xc-p2p)# neighbor 10.1.1.3 pw-id 1001 pw-class class13
RP/0/RP0/CPU0:router(config-xc-p2p)# rtrC_to_rtrD
RP/0/RP0/CPU0:router(config-xc-p2p)# neighbor 10.2.2.3 pw-id 200 pw-class class23
RP/0/RP0/CPU0:router(config-xc-p2p)# neighbor 10.2.2.4 pw-id 201 pw-class class24
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config) # 12vpn xconnect group 12vpn
RP/0/RP0/CPU0:router(config-12vpn-xc) # p2p rtrA_to_rtrB
RP/0/RP0/CPU0:router(config-xc-p2p) # neighbor 10.1.1.2 pw-id 1000 pw-class foo
RP/0/RP0/CPU0:router(config-xc) # p2p rtrC_to_rtrD
RP/0/RP0/CPU0:router(config-xc-p2p) # neighbor 20.2.2.3 pw-id 200 pw-class bar1
```

Command	Description
l2vpn, on page 44	Enters L2VPN configuration mode.
p2p, on page 65	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 138	Configures cross-connect groups.

# nsr (L2VPN)

To configure non-stop routing, use the **nsr** command in L2VPN configuration submode. To return to the default behavior, use the **no** form of this command.

nsr

no nsr

# **Syntax Description**

This command has no keywords or arguments.

# **Command Default**

None

#### **Command Modes**

L2VPN configuration submode

# **Command History**

Release	Modification
Release 4.3.0	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	Operation
12vpn	read, write

The following example shows how to configure non-stop routing:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# nsr

Command	Description
l2vpn, on page 44	Enters L2VPN configuration mode.

# 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.

 $\begin{array}{ll} password & [\{0 \mid 7\}] & password \\ no & password \end{array}$ 

#### **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 3.9.0	This command was introduced.

# **Usage Guidelines**

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

#### Task ID

Task ID	Operations
12vpn	read, write

# **Examples**

The following example shows how to define an unencrypted password using the word "cisco" for control channel authentication:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class sanjose
RP/0/RP0/CPU0:router(config-12tp-class)# password 0 cisco
```

Command	Description
authentication (L2TP), on page 11	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 28	Configures the hello-interval value for L2TP (duration between control channel hello packets).

Command	Description
hidden (L2TP), on page 30	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 32	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 36	Enters L2TP class configuration mode where you can define an L2TP signaling template.
receive-window (L2TP), on page 66	Configures the receive window size for the L2TP server.
retransmit (L2TP), on page 68	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
12vpn	read, write

#### **Examples**

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

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# xconnect group 11vpn
RP/0/RP0/CPU0:router(config-12vpn-xc)# p2p rtrA\_to\_rtrB
RP/0/RP0/CPU0:router(config-12vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-12vpn-xc-p2p-pw)# pw-class kanata01

Command	Description
p2p, on page 65	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 12tpv3 [{cookie size  $\{0 \mid 4 \mid 8\} \mid ipv4 \text{ source } address \mid pmtu max } 68-65535 \mid protocol 12tpv3 class } name \mid tos {reflect value } 0-255 \mid value } 0-255 \mid ttl value}]$  no pw-class class name encapsulation 12tpv3 [{cookie size }  $\{0 \mid 4 \mid 8\} \mid ipv4 \text{ source } address \mid pmtu max } 68-65535 \mid protocol 12tpv3 class } name \mid tos {reflect value } 0-255 \mid value } 0-255 \mid ttl value}]$ 

# **Syntax Description**

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

#### **Command Default**

None

#### **Command Modes**

L2VPN pseudowire class configuration

#### **Command History**

Release	Modification
Release 3.9.0	This command was introduced.

# **Usage Guidelines**

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



Note

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

Task ID	Task ID	Operations
	12vpn	read,
		write

# **Examples**

The following example shows how to define L2TPV3 pseudowire encapsulation:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# pw-class kanata01
RP/0/RP0/CPU0:router(config-12vpn-pwc)# encapsulation 12tpv3
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# pw-class kanata01
RP/0/RP0/CPU0:router(config-12vpn-pwc)# encapsulation 12tpv3
RP/0/RP0/CPU0:router(config-12vpn-pwc-12tpv3)# protocol 12tpv3
```

Command	Description
pw-class (L2VPN), on page 57	Enters pseudowire class submode to define a pseudowire class template.
pw-class encapsulation mpls, on page 60	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.

 $\label{load-balancing flow-label} $$ pw-class $$ class-name $$ encapsulation $$ mpls $$ \{control word | ipv4 | load-balancing flow-label | 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 | flow-label | preferred-path | protocol | ldp | sequencing | tag-rewrite | transport-mode | vccv | verification-type | none | ldp | sequencing | tag-rewrite | transport-mode | vccv | verification-type | none | ldp | ldp$ 

# **Syntax Description**

class-name	Encapsulation class name.
control word	Disables control word for MPLS encapsulation. Disabled by default.
ipv4	Sets the local source IPv4 address.
load-balancing flow-label	Sets flow label-based load balancing.
preferred-path	Configures the preferred path tunnel settings.
protocol ldp	Configures LDP as the signaling protocol for this pseudowire class.
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 <b>control word disable</b> and <b>vccv none</b> were replaced by the keywords <b>control word</b> and <b>vccv verification-type none</b> .

# Release Modification

Release 3.9.0 The following keywords were added:

- · preferred-path
- sequencing
- tag-rewrite
- · transport-mode

Release 4.3.0 The keyword **load-balancing flow-label** was introduced.

# **Usage Guidelines**

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



Note

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

#### Task ID

# Task Operations ID 12vpn read, write

# **Examples**

This example shows how to define MPLS pseudowire encapsulation:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# pw-class kanata01
RP/0/RP0/CPU0:router(config-12vpn-pwc)# encapsulation mpls
```

Command	Description
pw-class (L2VPN), on page 57	Enters pseudowire class submode to define a pseudowire class template.
pw-class encapsulation l2tpv3, on page 58	Configures L2TPv3 pseudowire encapsulation.

# pw-ether

To configure a PWHE Ethernet interface, use the **pw-ether** command in global configuration mode or in p2p configuration submode. To return to the default behavior, use the **no** form of this command.

pw-ether value
no pw-ether value

# **Syntax Description**

value Value of the PWHE Ethernet interface. The range is from 1 to 32768.

#### **Command Default**

None

#### **Command Modes**

Global configuration

p2p configuration

# **Command History**

Release	Modification
Release 4.2.1	This command was introduced.

#### **Usage Guidelines**

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

#### Task ID

Task ID	Operation
interface (global configuration)	read, write
l2vpn (p2p configuration)	read, write

This example shows the sample output of a PWHE Ethernet interface configuration in global configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface pw-ether 78
RP/0/RP0/CPU0:router(config-if)# attach generic-interface-list interfacelist1
```

This example shows the sample output of a PWHE Ethernet interface configuration in p2p configuration submode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# xconnect group xc1
RP/0/RP0/CPU0:router(config-12vpn-xc)#p2p grp1
RP/0/RP0/CPU0:router(config-12vpn-xc-p2p)#interface pw-ether 78
```

This example shows the sample output of L2 overhead configuration for the PW-HE interface:

RP/0/RP0/CPU0:router# configure

```
RP/0/RP0/CPU0:router(config) # interface pw-ether 78
RP/0/RP0/CPU0:router(config-if) # 12overhead 32
```

This example shows the sample output of Load-interval configuration for the PW-HE interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface pw-ether 78
RP/0/RP0/CPU0:router(config-if)# load-interval 60
```

This example shows the sample output of how to set logging of interface state change for the PW-HE interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface pw-ether 78
RP/0/RP0/CPU0:router(config-if)# logging events link-status
```

This example shows the sample output of MAC address configuration for the PW-HE interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface pw-ether 78
RP/0/RP0/CPU0:router(config-if)# mac-address 44-37-E6-89-C3-93
```

This example shows the sample output of MTU configuration for the PW-HE interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config) # interface pw-ether 78
RP/0/RP0/CPU0:router(config-if) # mtu 128
```

This example shows the sample output of bandwidth configuration for the PW-HE interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface pw-ether 78
RP/0/RP0/CPU0:router(config-if)# bandwidth 256
```

Command	Description
p2p, on page 65	Enters p2p configuration submode to configure point-to-point cross-connects.

# pw-grouping

To enable Pseudowire Grouping, use the **pw-grouping** command in L2vpn configuration submode. To return to the default behavior, use the **no** form of this command.

pw-grouping no pw-grouping

## **Syntax Description**

**pw-grouping** Enables Pseudowire Grouping.

## **Command Default**

PW-grouping is disabled by default.

#### **Command Modes**

L2VPN configuration submode

#### **Command History**

Release	Modification
Release 4.3.0	This command was introduced.

## **Usage Guidelines**

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

#### Task ID

Task ID	Operation
12vpn	read, write

This example shows the sample output of pw-grouping configuration in L2VPN configuration submode:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# pw-grouping

Command	Description
l2vpn, on page 44	Enters L2VPN configuration mode.
show I2vpn, on page 81	Displays L2VPN information

# 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.

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

#### Task ID

Task ID	Operations
12vpn	read, write

## **Examples**

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

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# xconnect group group 1
RP/0/RP0/CPU0:router(config-12vpn-xc)# p2p xc1

Command	Description
interface (p2p), on page 34	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 3.9.0	This command was introduced.

## **Usage Guidelines**

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

#### Task ID

Task ID	Operations
l2vpn	read, write

#### **Examples**

The following example shows how to configure the receive window size for the L2TP server to 10 packets:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class cisco
RP/0/RP0/CPU0:router(config-l2tp-class)# receive-window 10

Command	Description
authentication (L2TP), on page 11	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 28	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 30	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 32	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 36	Enters L2TP class configuration mode where you can define an L2TP signaling template.

Command	Description
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.
retransmit (L2TP), on page 68	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 3.9.0	This command was introduced.

## **Usage Guidelines**

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

## Task ID

Task ID	Operations
12vpn	read, write

#### **Examples**

The following example shows how to configure a retransmit retry value to 1:

RP/0/RP0/CPU0:router# configure

RP/0/RP0/CPU0:router(config)# 12tp-class cisco
RP/0/RP0/CPU0:router(config-12tp-class)# retransmit initial retries 1

Command	Description
authentication (L2TP), on page 11	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 28	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 30	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 32	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 36	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 66	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.

holddowntime Configures the holddown time for old session cookie values.

#### **Command Default**

None

#### **Command Modes**

tunnel encapsulation 12tp configuration

#### **Command History**

Kelease		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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# tunnel-template kanata\_9
RP/0/RP0/CPU0:router(config-tuntem) encapsulation 12tp
RP/0/RP0/CPU0:router(config-tunencap-12tp)# rollover

Command	Description	
interface (p2p), on page 34	Configures an attachment circuit.	

# show generic-interface-list

To display information about interface-lists, use the **show generic-interface-list** in EXEC mode.

show generic-interface-list [{ location | name | retry | standby }]

#### **Syntax Description**

location	(Optional) Displays information about interface-lists for the specified location.	
name	(Optional) Displays information about interface-lists for the specified interface list name.	
retry	(Optional) Displays retry-list information.	
standby	(Optional) Displays Standby node specific information.	

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

#### **Command History**

Release	Modification
Release 4.3.0	This command was introduced.

#### **Usage Guidelines**

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

#### Task ID

Task ID	Operation	
12vpn	read	

The following example displays output for the **show generic-interface-list** command:

```
RP/0/RP0/CPU0:router# show generic-interface-list
  Thu Aug 2 13:48:57.462 CDT
  generic-interface-list: nsrIL (ID: 1, interfaces: 2)
    Bundle-Ether2 - items pending 0, downloaded to FIB
    GigabitEthernet0/0/0/1 - items pending 0, downloaded to FIB
  Number of items: 400
  List is downloaded to FIB
```

The following example displays output for the **show generic-interface-list retry private** command:

```
RP/0/RP0/CPU0:router# show generic-interface-list retry private
Thu Aug 2 14:20:42.883 CDT
total: 0 items
```

The following example displays output for the **show generic-interface-list standby** command:

RP/0/RP0/CPU0:router# show generic-interface-list standby

Thu Aug 2 14:25:01.749 CDT generic-interface-list: nsrIL (ID: 0, interfaces: 2) Bundle-Ether2 - items pending 0, NOT downloaded to FIB GigabitEthernet0/0/0/1 - items pending 0, NOT downloaded to FIB Number of items: 0 List is not downloaded to FIB

Command	Description	
I2vpn, on page 44	Enters L2VPN configuration mode.	

# show l2tp class

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

show 12tp class name name

Syntax Description	name	Configures an L2TP class name.
	name	

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

## **Command History**

Release	Modification
Release 3.9.0	This command was introduced.

#### **Usage Guidelines**

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

#### Task ID

Task ID	Operations
12vpn	read, write

## **Examples**

The following example shows sample output for the **show l2vtp session class** command:

```
RP/0/RP0/CPU0:router# show 12tp class name kanata 02
12tp-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
```

```
\begin{tabular}{ll} retransmit initial timeout min 1 \\ timeout setup 300 \\ \end{tabular}
```

This table describes the significant fields shown in the display.

# Table 1: show I2tp class brief Field Descriptions

Field	Description
12tp-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.

Command	Description
l2tp-class, on page 36	Enters L2TP class configuration mode where you can define an L2TP signaling template.

# show I2tp counters forwarding session

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

show 12tp 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
neiease	woullication

Release 3.9.0 This command was introduced.

#### **Usage Guidelines**

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

#### Task ID

Task ID	Operations
l2vpn	read,
	write

#### **Examples**

The following example shows sample output for the **show l2tp counters forwarding session** command:

RP/0/RP00/CPU0:router(config-12vpn)# pw-class kanata01show 12tp counters
forwarding session

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

This table describes the significant fields shown in the display.

#### Table 2: show I2tp counters forwarding session Field Descriptions

Field	Description
LocID	Local session ID.
RemID	Remote session ID.
TunID	Local Tunnel ID for this session.

Field	Description
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.

Command	Description
#unique_59	

# show l2tp session

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

show 12tp 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 3.9.0	This command was introduced.

#### **Usage Guidelines**

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

#### Task ID

Task ID	Operations
l2vpn	read, write

## **Examples**

The following sample output is from the **show l2tp session brief** command:

RP/0/RP00/CPU0:router(config-12vpn-pw) # show 12tp session brief
Tue Jun 10 12:51:30.901 UTC
LocID TunID Peer-address State Username, Intf/sess/cir Vcid, Circuit
1606803058 1487464659 26.26.26 est,UP 101, Gi0/2/0/1.101
3663696887 1487464659 26.26.26.26 est,UP 100, Gi0/2/0/1.100

This table describes the significant fields shown in the display.

#### Table 3: show I2tp 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.
Veid	The Virtual Circuit ID of the session. This is the same value of the pseudowire ID for l2vpn.

The following sample output is from the **show l2tp session detail** command:

```
RP/0/RP00/CPU0:router(config-12vpn-pw)# show l2tp session detail
Tue Jun 10 12:53:19.842 UTC
Session id 1606803058 is up, tunnel id 1487464659, logical session id 131097
 Remote session id is 2602674409, remote tunnel id 2064960537
 Remotely initiated session
Call serial number is 4117500017
Remote tunnel name is ASR9K-PE2
  Internet address is 26.26.26.26:1248
Local tunnel name is PRABHRAM-PE1
 Internet address is 25.25.25.25:4272
IP protocol 115
 Session is L2TP signaled
  Session state is established, time since change 00:07:28
 UDP checksums are disabled
 Session cookie information:
   local cookie, size 4 bytes, value 6d 3e 03 67
   remote cookie, size 4 bytes, value 0d ac 7a 3b
  Tie breaker is 0xfee65781a2fa2cfd, enabled TRUE.
  Sequencing is off
  Conditional debugging is disabled
 Unique ID is 101
Session Layer 2 circuit
 Payload type is Ethernet, Name is GigabitEthernet0 2 0 1.101
  Session vcid is 101
  Circuit state is UP
   Local circuit state is UP
   Remote circuit state is UP
```

Command	Description
#unique_59	

# show I2tp tunnel

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

show 12tp 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 3.9.0	This command was introduced.

# **Usage Guidelines**

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

#### Task ID

Task ID	Operations
12vpn	read, write

#### **Examples**

The following sample output is from the **show l2tp tunnel brief** command:

RP/0/RP0/CPU0:router(config-l2vpn-encap-mpls)# show 12tp tunnel brief
Tue Jun 10 12:46:04.421 UTC
LocTunID RemTunID Remote Name State Vrf Name Remote Address Sessn L2TP Class/Count
VPDN Group
1487464659 2064960537 ASR9K-PE2 est 26.26.26.26 2 L2TPV3\_CLASS

This table describes the significant fields shown in the display.

#### Table 4: show I2tp tunnel Field Descriptions

Field	Description
LocTunID	Local session ID.
RemTunID	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.

#### The following sample output is from the **show l2tp tunnel detail** command:

```
RP/0/RP0/CPU0:router(config-12vpn-encap-mpls)# show 12tp tunnel detail
Tue Jun 10 12:47:36.638 UTC
Tunnel id 1487464659 is up, remote id is 2064960537, 2 active sessions
 Remotely initiated tunnel
  Tunnel state is established, time since change 4d19h
 Tunnel transport is IP (115)
 Remote tunnel name is ASR9K-PE2
   Internet Address 26.26.26.26, port 0
  Local tunnel name is PRABHRAM-PE1
   Internet Address 25.25.25.25, port 0
  VRF table id is 0xe0000000
  Tunnel group id
  L2TP class for tunnel is L2TPV3_CLASS
  Control Ns 4178, Nr 4181
  Local RWS 512 (default), Remote RWS 512
  Control channel Congestion Control is disabled
  Tunnel PMTU checking disabled
  Retransmission time 1, max 1 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 1
  Total resends 0, ZLB ACKs sent 4177
  Total out-of-order dropped pkts 0
  Total out-of-order reorder pkts 0
  Total peer authentication failures 0
  Current no session pak queue check 0 of 5
  Retransmit time distribution: 0 0 0 0 0 0 0 0 0
  Control message authentication is disabled
```

Command	Description
show I2tp session, on page 77	Displays information about L2TP sessions.

# show I2vpn

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

#### show 12vpn

## **Syntax Description**

This command has no keywords or arguments.

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

## **Command History**

Release	Modification
Release 4.3.0	This command was introduced.

## **Usage Guidelines**

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

## Task ID

Task ID	Operation
12vpn	read

# Example

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

```
RP/0/RP0/CPU0:router# show 12vpn
Mon May 7 15:01:17.963 BST
PW-Status: disabled
PW-Grouping: disabled
Logging PW: disabled
Logging BD state changes: disabled
Logging VFI state changes: disabled
Logging NSR state changes: disabled
TCN propagation: disabled
PWOAMRefreshTX: 30s
```

Command	Description
I2vpn, on page 44	Enters L2VPN configuration mode.
pw-grouping, on page 64	Enables Pseudowire Grouping

# show I2vpn atom-db

To display AToM database information, use the **show l2vpn atom-db** command in EXEC mode.

show 12vpn atom-db [{detail | 12-rid | ldp-rid | local-gid | neighbor | preferred-path | remote-gid | source}]

## **Syntax Description**

detail	Specifies the details of the database.
12-rid	Specifies the AToM database walking the L2 RID thread.
ldp-rid	Specifies the AToM database walking the LDP RID thread.
local-gid	Specifies the AToM database walking the Local GID thread.
neighbor	Specifies the details of the neighbor database.
preferred-path	Specifies the preferred path (tunnel) of the database
remote-gid	Specifies the AToM database walking the Remote GID thread.
source	Specifies the details of the source database.

#### **Command Default**

None

## **Command Modes**

**EXEC** 

# **Command History**

Release	Modification
Release 4.2.1	This command was introduced.

## **Usage Guidelines**

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

## Task ID

Task ID	Operations
l2vpn	read

## **Examples**

This example shows the sample output of the **show l2vpn atom-db source 1.1.1.1** command:

RP/U/RPU/CPU	0:router# <b>show</b>	12vpn atom-db	source	1.1.1.1		
Peer ID	Source	VC ID	Encap	Signaling	FEC	Discovery
2.2.2.2	1.1.1.1	1	MPLS	LDP	128	none

This example shows the sample output of the show l2vpn atom-db source 1.1.1.1 detail command:

```
RP/0/RP0/CPU0:router# show l2vpn atom-db source 1.1.1.1 detail
 PW: neighbor 2.2.2.2, PW ID 1, state is down (provisioned)
   PW class class1, XC ID 0x1
   Encapsulation MPLS, protocol LDP
   Source address 1.1.1.1
   PW type Ethernet, control word disabled, interworking none
   PW backup disable delay 0 sec
   Sequencing not set
                Local
                                               Remote
     ______
     Label
                 16000
                                               unknown
     Group ID 0x20000060
                                               0x0
     Interface GigabitEthernet0/0/0/1.1
                                             unknown
                1504
                                              unknown
     Control word disabled
                                               unknown
     PW type Ethernet
                                               unknown
     VCCV CV type 0x2
                                                0x0
                                                (none)
                  (LSP ping verification)
     VCCV CC type 0x6
                                               0x0
                                                (none)
                  (router alert label)
                  (TTL expiry)
   MIB cpwVcIndex: 4278194081
   Create time: 13/12/2010 15:28:26 (20:32:27 ago)
   Last time status changed: 13/12/2010 15:28:26 (20:32:27 ago)
   Configuration info:
     PW class: class1
     Peer ID = 2.2.2.2, pseudowire ID = 1
     Control word is not set
     Transport mode: not set
       Configured (Static) Encapsulation: not set
       Provisioned Encapsulation: MPLS
     Static tag rewrite: not set
     MTU: 1504
     Tunnel interface: None
     IW type: 0
     PW type: Dynamic
     Pref path configured: No
     Bridge port: No
     BP learning disabled: No
     BP ucast flooding disabled: No
     BP bcast flooding disabled: No
     CW is mandatory: No
     Label: local unassigned, remote unassigned
     L2 Router-ID: 0.0.0.0
     LDP Router-ID: 0.0.0.0
     GR stale: No
   LDP Status: local established, remote unknown
   LDP tag rewrite: not set
   Force switchover: inactive
   MAC trigger: inactive
   VC sane: Yes
   Use PW Status: No
   Local PW Status: Up(0x0); Remote PW Status: Up(0x0)
   Peer FEC Failed: No
   LSP: Down
   Operational state:
     LDP session state: down
     TE tunnel transport: No
     VC in gr mode: No
     Peer state: up
```

0x3e80

0x5e0

Transport LSP down: Yes
Advertised label to LDP: No
Received a label from LSD: Yes
Need to send standby bit: No
VC created from rbinding: No
PW redundancy dampening on : No
Notified up : No
Detailed segment state: down
PW event trace history [Total events: 8]

12/13/2010 15:28:26 Got label

12/13/2010 15:28:26 Local Mtu

12/13/2010 15:28:26 Peer Up

# show I2vpn 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 12vpn collaborators

## **Syntax Description**

This command has no arguments or keywords.

## **Command Default**

None

#### **Command Modes**

**EXEC** 

#### **Command History**

Kelease	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
12vpn	read, write

## **Examples**

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

RP/0/RP0/CPU0:router# show 12vpn 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 I2vpn collaborators Field Descriptions

Field	Description
Name	Abbreviated name of the task interacting with 12vpn_mgr.
State	Indicates if 12vpn_mgr has a working connection with the other process.
Up Cnts	Number of times the connection between l2vpn_mgr and the other process has been successfully established.

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

Command	Description
clear l2vpn collaborators, on page 18	Clears the state change counters for L2VPN collaborators.

# show I2vpn database

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

show 12vpn database {ac | node}

#### **Syntax Description**

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

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

#### **Command History**

Release	Modification
Release 4.3.0	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.

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

## Task ID

Task ID	Operation
12vpn	read

The following example displays output for the show 12vpn database ac command:

```
RP/0/RP0/CPU0:router# show 12vpn database ac
    Bundle-Ether1.1:
          Other-Segment MTU: 0
          Other-Segment status flags: 0x0
          Signaled capability valid: No
          Signaled capability flags: 0x0
          Configured capability flags: 0x0
          XCID: 0xffffffff
          PSN Type: Undefined
          ETH data:
              Xconnect tags: 0
              Vlan rewrite tag: 0
        AC defn:
            ac-ifname: Bundle-Ether1.1
            capabilities: 0x00368079
            extra-capabilities: 0x00000000
            parent-ifh: 0x020000e0
            ac-type: 0x15
            interworking: 0x00
        AC info:
```

```
seg-status-flags: 0x00000000
       segment mtu/12-mtu: 1504/1518
GigabitEthernet0/0/0/0.4096:
     Other-Segment MTU: 0
     Other-Segment status flags: 0x0
      Signaled capability valid: No
     Signaled capability flags: 0x0
     Configured capability flags: 0x0
     XCID: 0x0
     PSN Type: Undefined
     ETH data:
         Xconnect tags: 0
         Vlan rewrite tag: 0
   AC defn:
       ac-ifname: GigabitEthernet0 0 0 0.4096
       capabilities: 0x00368079
       extra-capabilities: 0x00000000
       parent-ifh: 0x040000c0
       ac-type: 0x15
       interworking: 0x00
   AC info:
       seg-status-flags: 0x00000003
        segment mtu/12-mtu: 1504/1518
```

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

```
RP/0/RP0/CPU0:router# show 12vpn database node
   0/RSP0/CPU0
      MA: vlan ma
       AC event trace history [Total events: 4]
              Event
                                                Num Rcvd
                                                             Num Sent
                       =====
                                                _____
                                                              _____
       07/27/2012 15:00:31 Process joined
                                                             0
                                                             Ω
       07/27/2012 15:00:31 Process init success
                                               0
       07/27/2012 15:00:31 Replay start rcvd
                                                0
                                                              0
       07/27/2012 15:00:31 Replay end rcvd
      MA: ether ma
       AC event trace history [Total events: 4]
       _____
       Time
                                                             Num Sent
                                                Num Rayd
                      Event
                       =====
                                                              =======
       07/27/2012 15:00:31 Process joined
                                                0
                                                              0
                                               0 0
       07/27/2012 15:00:31 Process init success
                                                              0
       07/27/2012 15:00:31 Replay start rcvd
                                                              0
       07/27/2012 15:00:31 Replay end rcvd
                                                             Ω
   0/0/CPU0
      MA: vlan ma
       AC event trace history [Total events: 4]
       ______
       Time
                       Event.
                                                Num Ravd
                                                         Num Sent
                                                 =======
                       =====
                                                              _____
       07/27/2012 15:00:31 Process joined
                                                 Ω
                                                              Ω
       07/27/2012 15:00:31 Process init success
                                               0
                                                             0
       07/27/2012 15:00:31 Replay start rcvd
                                               0
                                                             0
```

07/27/2012 15:00:40 Replay end rcvd

6006

6001

MA: ether\_ma

AC event trace history [Total events: 4]

-----

Time	Event	Num Rcvd	Num Sent
====	=====	======	=======
07/27/2012 15:00:31	Process joined	0	0
07/27/2012 15:00:31	Process init success	0	0
07/27/2012 15:00:31	Replay start rcvd	0	0
07/27/2012 15:00:31	Replay end rcvd	1	0

# show I2vpn forwarding

To display forwarding information from the layer2\_fib manager on the line card, use the **show l2vpn forwarding** command in EXEC mode.

show 12vpn forwarding {xconnect | bridge-domain | counter | detail | hardware | inconsistent | interface | 12tp | location [node-id] | message | mstp | resource | retry-list | summary | unresolved}

## **Syntax Description**

xconnect	Displays the cross-connect related information.
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.
12tp	Displays L2TPv3 related forwarding information.
location node-id	Displays layer2_fib manager information for the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> 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 commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

#### Task ID

# Task Operations ID

l2vpn read

#### **Examples**

The following sample output is from the **show l2vpn forwarding bridge detail location** command for IOS-XR releases 5.3.1 and earlier:

```
RP/0/RP0/CPU0:router# show 12vpn forwarding bridge detail 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 output is from the **show l2vpn forwarding bridge detail location** command for IOS-XR 5.3.2 release:

```
RP/0/RP0/CPU0:router# show 12vpn forwarding bridge detail location 0/0/CPU0
Bridge-domain name: pbb:pbb_core1, id: 10, state: up
Type: pbb-core
Number of associated pbb-edge BDs: 1
```

```
MAC learning: enabled
MAC port down flush: enabled
Flooding:
  Broadcast & Multicast: enabled
  Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC Secure: disabled, Logging: disabled
DHCPv4 snooping: profile not known on this node
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
IGMP snooping: disabled, flooding: enabled
MLD snooping: disabled, flooding: disabled
MMRP Flood Optimization: disabled
Storm control: disabled
P2MP PW: disabled
Bridge MTU: 1500 bytes
Number of bridge ports: 1
Number of MAC addresses: 5
Multi-spanning tree instance: 0
PBB-EVPN: enabled
Statistics:
  packets: received 0, sent 963770
  bytes: received 0, sent 263433178
 PBB Core, state: Up
   Vlan-id: 1
   XC ID: 0x80000010
   Number of MAC: 0
   Statistics:
     packets: received 0 (unicast 0), sent 0
     bytes: received 0 (unicast 0), sent 0
     MAC move: 0
   Storm control drop counters:
     packets: broadcast 0, multicast 0, unknown unicast 0
     bytes: broadcast 0, multicast 0, unknown unicast 0
```

The following sample outputs shows the backup pseudowire information:

```
RP/0/RP0/CPU0:router#show 12vpn forwarding detail location 0/2/CPU0
Local interface: GigabitEthernet0/2/0/0.1, Xconnect id: 0x3000001, Status: up
  Seament 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/RP0/CPU0:router#show 12vpn 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
RP/0/RP0/CPU0:router#show 12vpn 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
XC ID: 0x1880002
Number of MAC: 0
Statistics:
packets: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent 963770
bytes: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent 263433178
MAC move: 0
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
The following sample outputs displays the SPAN segment information of the xconnect:
RP/0/RP0/CPU0:router# show 12vpn forwarding counter location 0/7/CPU0
Legend: ST = State, DN = Down
                                   Segment 2
                                                    ST
Seament 1
                                                          Bvte
                                                                          Switched
______
                                                            -----
pw-span-test (Monitor-Session) mpls 2.2.2.2 UP
RP/0/RP0/CPU0:router #Show 12vpn forwarding monitor-session location 0/7/CPU0
Segment 1
                    Segment 2
pw-span-test(monitor-session) mpls 2.2.2.2
                                                             ΠP
pw-span-sess(monitor-session) mpls 3.3.3.3
                                                               ΠP
RP/0/RP0/CPU0:router #Show 12vpn forwarding monitor-session pw-span-test location 0/7/CPU0
Segment 1
                            Segment 2
pw-span-test(Monitor-Session) mpls 2.2.2.2
                                                            UP
RP/0/RP0/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
show 12vpn 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]
          Event Flags
   Time
                       ____
RP/0/RP0/CPU0:router #show 12vpn 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:

#### The following sample output shows the MAC information in the layer2\_fib manager summary:

```
RP/0/RP0/CPU0:router# show 12vpn forwarding summary location 0/3/CPU0
Major version num:1, minor version num:0
Shared memory timestamp:0x66ff58e894
Number of forwarding xconnect entries:2
Up:1 Down:0
AC-PW:0 AC-AC:0 AC-BP:1 PW-BP:1
Number of xconnects down due to:
AIB:0 L2VPN:0 L3FIB:0
Number of nexthops:1
Number of static macs: 5
Number of locally learned macs: 5
Number of remotely learned macs: 0
Number of total macs: 10
```

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

```
RP/0/RP0/CPU0:router# show 12vpn for 0/0/cPU0
Local interface: GigabitEthernet0/0/1/1, Xconnect id: 0x1000002, Status: up
  Seament 1
   AC, GigabitEthernet0/0/1/1, Ethernet port mode, status: Bound
  Segment 2
   MPLS, Destination address: 3.3.3, pw-id: 2, status: Bound, Active
    Pseudowire label: 16004 Control word disabled
     MPLS, Destination address: 2.2.2.2, pw-id: 6, status: Bound
     Pseudowire label: 16000
    Flow label enabled
    Xconnect id: 0xff000014, Status: down
  Seament 1
   MPLS, Destination address: 2.2.2.2, pw-id: 1, status: Not bound
  Pseudowire label: UNKNOWN Control word disabled
   Flow label enabled
  Segment 2
   Bridge id: 0, Split horizon group id: 0
    Storm control: disabled
   MAC learning: enabled
   MAC port down flush: enabled
   Flooding:
     Broadcast & Multicast: enabled
     Unknown unicast: enabled
   MAC aging time: 300 s, Type: inactivity
   MAC limit: 4000, Action: none, Notification: syslog
   MAC limit reached: no
    Security: disabled
   DHCPv4 snooping: profile not known on this node, disabled
```

 ${\tt IGMP}$  snooping profile: profile not known on this node  ${\tt Router}$  guard disabled

Command	Description
clear I2vpn forwarding counters, on page 21	Clears L2VPN forwarding counters.

# show I2vpn forwarding I2tp

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

show 12vpn forwarding 12tp 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 3.9.0	This command was introduced.

# **Usage Guidelines**

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

#### Task ID

Task ID	Operations
12vpn	read

## **Examples**

The following example shows sample output for the **show l2vpn forwarding l2tp** command:

 ${\tt RP/0/RP0/CPU0:} router \# show 12 vpn forwarding 12 tp disposition hardware location 0/3/1$ 

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

Command	Description
clear I2vpn forwarding counters, on page 21	Clears L2VPN forwarding counters.

## show I2vpn generic-interface-list

To display all the L2VPN virtual interfaces, use the **show l2vpn generic-interface-list** command in EXEC mode.

## **Syntax Description**

detail	Specifies the details of the interface.
name	Specifies the name of the interface.
private	Specifies the private details of the interface.
summary	Specifies the summary information of the interface.

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

#### **Command History**

Release	Modification
Release 4.2.1	This command was introduced.

## **Usage Guidelines**

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

#### Task ID

Task ID	Operations
12vpn	read

### **Examples**

This example shows the sample output of the **show l2vpn generic-interface-list** command:

```
RP/0/RP0/CPU0:router# show l2vpn generic-interface-list
generic-interface-list: 11 (ID: 2, interfaces: 2) Number of items: 20
generic-interface-list: 12 (ID: 3, interfaces: 4) Number of items: 15
```

This example shows the sample output of the show l2vpn generic-interface-list detail command:

```
RP/0/RP0/CPU0:router# show l2vpn generic-interface-list detail
generic-interface-list: l1 (ID: 2, interfaces: 2)
   GigabitEthernet0/1/0/0 - items pending 2
   GigabitEthernet0/1/0/1 - items pending 4
   Number of items: 27
   PW-Ether: 1-10, 12-21
   PW-IW: 1-7
generic-interface-list: l2 (ID: 3, interfaces: 4)
```

```
GigabitEthernet0/1/0/0 - items pending 2
GigabitEthernet0/1/0/1 - items pending 4
GigabitEthernet0/1/0/2 - items pending 1
GigabitEthernet0/1/0/3 - items pending 0
Number of items: 20
PW-Ether: 1-15
PW-IW: 1-7
```

This example shows the sample output of the **show l2vpn generic-interface-list name** | **detail** command:

```
RP/0/RP0/CPU0:router# show l2vpn generic-interface-list name 11 detail
generic-interface-list: l1 (ID: 2, interfaces: 2)
   GigabitEthernet0/1/0/0 - items pending 2
   GigabitEthernet0/1/0/1 - items pending 4
   Number of items: 20
   PW-Ether 1-10, 12-21
```

## show I2vpn index

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

show 12vpn index [{location | private | standby}]

## **Syntax Description**

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

#### **Command Default**

None

## **Command Modes**

**EXEC** 

## **Command History**

Release	Modification
Release 4.2.1	This command was introduced.
Release 4.3.0	The following keywords are introduced:

## **Usage Guidelines**

To use this command, you must be in a user group associated with a task 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
12vpn	read

## **Examples**

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

```
RP/0/RP0/CPU0:router# show 12vpn index
Pool id: 0x4, App: RD
Pool size: 32767
zombied IDs: 0
allocated IDs: 0
Pool id: 0x5, App: IFLIST
```

```
Pool size: 65535
zombied IDs: 0
allocated IDs: 2

Pool id: 0xff000001, App: PW/PBB/Virtual AC
Pool size: 40960
zombied IDs: 0
allocated IDs: 1

Pool id: 0xff000002, App: BD
Pool size: 4095
zombied IDs: 0
allocated IDs: 2

Pool id: 0xff000003, App: MP2MP
Pool size: 65535
zombied IDs: 0
allocated IDs: 0
allocated IDs: 1
```

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

```
RP/0/RP0/CPU0:router# show 12vpn index standby
   Pool id: 0xfffc0000, App: Global
     Max number of ID mgr instances: 1
      ID mgr instances in use: 1
      Pool size: 98304
      zombied IDs: 0
      allocated IDs: 0
    Pool id: 0xfffc0002, App: BD
      Max number of ID mgr instances: 1
      ID mgr instances in use: 1
      Pool size: 8192
      zombied IDs: 0
      allocated IDs: 0
    Pool id: 0xfffc0003, App: MP2MP
      Max number of ID mgr instances: 1
      ID mgr instances in use: 1
      Pool size: 65535
      zombied IDs: 0
      allocated IDs: 0
```

## show I2vpn nsr

To display the status of 12vpn non-stop routing, use the **show 12vpn nsr** command in EXEC mode.

show l2vpn nsr [{location | standby}]

#### **Syntax Description**

location	(Optional) Displays non-stop routing information for the specified location.
standby	(Optional) Displays Standby node specific information.

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

#### **Command History**

Release	Modification
Release 4.3.0	This command was introduced.
Release 6.1.2	The show command output was updated.

#### **Usage Guidelines**

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

#### Task ID

Task ID	Operation
l2vpn	read

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

```
RP/0/RP0/CPU0:router# show 12vpn nsr
```

```
Mon May 30 19:32:01.045 UTC
L2VPN NSR information
 NSR Status:
                           : Fri May 27 10:50:59 UTC 2016 (3d08h ago)
   NSR Ready
    Last NSR Withdraw Time : Fri May 27 10:50:59 UTC 2016 (3d08h ago)
   Standby Connected : Fri May 27 10:50:59 UTC 2016 (3d08h ago)
    IDT Done
                           : Fri May 27 10:50:59 UTC 2016 (3d08h ago)
   Number of XIDs sent
                            : Virtual AC: 0
                              AC
                              BD
                                        : 0
                              MP2MP
                                        : 0
                              RD
                              PBB
                                        : 0
                              IFLIST
                                       : 0
                              MOTA
                                       : 1
                              Global
```

PWGroup : 0 EVPN : 0

Command	Description
I2vpn, on page 44	Enters L2VPN configuration mode.
nsr (L2VPN), on page 54	Configures non-stop routing.

## show I2vpn process fsm

To display the status of the l2vpn process finite state machine, use the **show l2vpn process fsm** command in EXEC mode. It displays the current process role and state, NSR status, ISSU status, role change status, and status of collaborators.

show 12vpn process fsm [{location | standby}]

## **Syntax Description**

location	(Optional) Displays non-stop routing information for the specified location.
standby	(Optional) Displays Standby node specific information.

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

#### **Command History**

Release	Modification
Release 6.1.2	This command was introduced.

## **Usage Guidelines**

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

### Task ID

Task ID	Operation
12vpn	read

The following example displays output for the show l2vpn process fsm command:

RP/0/RP0/CPU0:router# show 12vpn process fsm

```
Mon May 16 10:20:30.967 PDT
L2VPN Process FSM
  Current process role
                           : Primary Active (Master)
  Current process state
                           : Run
  S/w install in progress : No
  NSR Status:
   NSR Readv
                           : No
   Last NSR Withdraw Time : Mon May 16 10:19:58 PDT 2016 (00:00:33 ago)
    Standby Connected
                           : No
   IDT Done
                           : Never
    Number of XIDs sent
                           : Virtual AC: 0
                             AC
                              PW
                                       : 1
                              BD
                             MP2MP
                             RD
                                       : 0
                              PBB
                                       : 0
                              TFLIST
```

```
MOTA
                                      : 1
                             Global
                                      : 0
                             PWGroup
                                     : 0
                             EVPN
 Process Role Change Status:
   Role Change Triggered : No Role Change
                       : No
: No
   Role Change Start
   Role Change End
 Process State Transition Time:
                          : Mon May 16 10:19:29 PDT 2016 (00:01:02 ago)
   Process-Start
                          : Mon May 16 10:19:30 PDT 2016 (00:01:01 ago)
   Process-Init
   Role-based Init
                          : Mon May 16 10:19:31 PDT 2016 (00:01:00 ago)
   Wait-Collab-Conn
                           : Mon May 16 10:19:31 PDT 2016 (00:01:00 ago)
                          : Mon May 16 10:19:58 PDT 2016 (00:00:33 ago)
 Process Collaborator Report Card:
                                                                              IDT Done
   Collaborator Connection Status (Since)
(At)
                       Up (Mon May 16 10:19:30 PDT 2016 (00:01:01 ago))
   NSR-INFRA
                                                                              N/A
   NSR-PEER
                       Down (Never came Up)
                                                                              Nο
   ISSU-PEER
                       Down (Never came Up)
                                                                              No
                    Up (Mon May 16 10:19:30 PDT 2016 (00:01:01 ago))
                                                                              Mon May 16
   SYSDB-CONFIG
10:19:58 PDT 2016 (00:00:33 ago)
```

Command	Description
I2vpn, on page 44	Enters L2VPN configuration mode.
nsr (L2VPN), on page 54	Configures non-stop routing.
show I2vpn index, on page 101	Displays statistics about the index manager.

## show I2vpn provision queue

To display L2VPN configuration provisioning queue information, use the **show l2vpn provision queue** command in EXEC mode.

show 12vpn provision queue [{location | standby}]

## **Syntax Description**

**location** (Optional) Displays L2VPN configuration provisioning queue information for the specified location.

standby (Optional) Displays Standby node specific information.

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

#### **Command History**

Release	Modification
Release 4.3.0	This command was introduced.

## **Usage Guidelines**

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

### Task ID

Task ID	Operation
12vpn	read

The following example displays output for the **show l2vpn provision queue** command:

RP/0/RP0/CPU0:router# show 12vpn provision queue

Legend: $P/P/R = Pri$	iority/Provisioned/Require	Provisioning.	
Configuration Item	Object Type	Class	P/P/R Object
Key			
BD_NAME	bd_t	vpls_bd_class	0/0/0 BD
VPLS01			
BD_NAME	bd_t	vpls_bd_class	0/0/0 BD
VPLS02			
BD NAME	bd t	vpls bd class	0/0/0 BD
VPIS03	<del>-</del>		

The following example displays output for the show 12vpn provision queue standby command:

RP/0/RP0/CPU0:router# show 12vpn provision queue standby

Legend: P/P/R = Priority/Provisioned/Require Provisioning.
Configuration Item Object Type Class

P/P/R Object

BD_NAME VPLS01	bd_t	vpls_bd_class	0/0/0 B	D
BD_NAME VPLS02	bd_t	vpls_bd_class	0/0/0 B	D
BD_NAME VPLS03	bd_t	vpls_bd_class	0/0/0 B	D
BD_NAME VPLS04	bd_t	vpls_bd_class	0/0/0 B	D
BD_NAME	bd_t	vpls_bd_class	0/0/0 B	D
VPLS05  BD_NAME  VPLS06	bd_t	vpls_bd_class	0/0/0 B	D
BD_NAME VPLS07	bd_t	vpls_bd_class	0/0/0 B	D
BD_NAME VPLS08	bd_t	vpls_bd_class	0/0/0 B	D
BD_NAME VPLS09	bd_t	vpls_bd_class	0/0/0 B	D
BD_NAME VPLS010	bd_t	vpls_bd_class	0/0/0 B	D

Command	Description
l2vpn, on page 44	Enters L2VPN configuration mode.

## show I2vpn pw-class

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

show 12vpn pw-class [{detail | location | name | class | name | standby}]

#### **Syntax Description**

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

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

### **Command History**

Release	Modification
Release 3.5.0	This command was introduced.
Release 4.3.0	The keywords <b>location</b> and <b>standby</b> were introduced.

### **Usage Guidelines**

To use this command, you must be in a user group associated with a task 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/RP0/CPU0:router# show 12vpn pw-class

Name	Encapsulation	Protocol
mplsclass_75	MPLS	LDP
12tp-dynamic	L2TPv3	L2TPv3

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

```
RP/0/RP0/CPU0:router# show 12vpn pw-class detail
```

```
Encapsulation MPLS, protocol LDP
Transport mode not set, control word unset (default)
Sequencing not set
Static tag rewrite not set
```

```
PW Backup disable delay: 0 sec
MAC withdraw message is sent over PW: no
IPv4 source address 1.1.1.1
```

This table describes the significant fields shown in the display.

## Table 6: show I2vpn 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.

Command	Description
clear I2vpn forwarding counters, on page 21	Clears L2VPN forwarding counters.

## show I2vpn pwhe

To display the pseudowire headend (PWHE) information, use the **show l2vpn pwhe** command in EXEC mode.

show 12vpn pwhe {detail | interface | summary}

## **Syntax Description**

detail	Specifies the details of the interface.	
interface	Specifies the name of the interface.	
summary	Specifies the summary information of the interface.	

#### **Command Default**

None

#### **Command Modes**

**EXEC** 

#### **Command History**

Release	Modification
Release 4.2.1	This command was introduced.

## **Usage Guidelines**

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

#### Task ID

Task ID	Operations
l2vpn	read

#### **Examples**

This example show the sample output for **show l2vpn pwhe detail** command:

```
RP/0/RP0/CPU0:router# show 12vpn pwhe detail
Interface handle 0x20000070
 MTU: 1514
 BW: 10000 Kbit
 Interface MAC addresses: 0279.96e9.8205
 Label: 16000
 L2-overhead: 0
 VC-type: 5
 CW: N
 Generic-interface-list: ifl1 (id: 1)
  Gi0/2/0/1, in bundle BE3, state: Up, replication: success
  Gi0/2/0/0, in bundle BE5, state: Up, replication: success
  Gi0/2/0/2, in bundle BE5, state: Up, replication: success
  Gi0/2/0/3, state: Up, replication: success
Interface: PW-IW1 Interface State: Up, Admin state: Up
 Interface handle 0x20000070
```

```
MTU: 1514
BW: 10000 Kbit
VC-type: 11
CW: N
Generic-interface-list: ifl2 (id: 2)
Gi0/3/0/1, in bundle BE6, state: Up, replication: success
Gi0/3/0/2, state: Up, replication: success
Gi0/3/0/3, state: Up, replication: success
```

This example show the sample output for show l2vpn pwhe summary command:

```
RP/0/RP0/CPU0:router# show 12vpn pwhe summary
Number of PW-HE interface: 1600
Up: 1300 Down: 300 Admindown: 0
Number of PW-Ether interfaces: 900
Up: 700 Down: 200 Admindown: 0
Number of PW-IW interfaces: 700
Up: 600 Down: 100 Admindown: 0
```

## show I2vpn resource

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

#### show 12vpn 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
12vpn	read

## **Examples**

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

RP/0/RP0/CPU0:router# show 12vpn resource

Memory: Normal

describes the significant fields shown in the display. Table 7: show l2vpn resource Command Field Descriptions, on page 113

### Table 7: show I2vpn resource Command Field Descriptions

Field	Description
Memory	Displays memory status.

## show I2vpn trace

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

show 12vpn trace [{checker|file|hexdump|last|location|reverse|stats|tailf|unique|usec|verbose|wide|wrapping}]

## **Syntax Description**

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

## **Command Default**

None

## **Command Modes**

**EXEC** 

## **Command History**

Release	Modification
Release 4.3.0	This command was introduced.

## **Usage Guidelines**

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

## Task ID

Task ID	Operation
l2vpn	read

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

```
RP/0/RP0/CPU0:router# show 12vpn trace
    310 unique entries (1775 possible, 0 filtered)
    Jul 27 14:39:51.786 l2vpn/fwd-detail 0/RSP0/CPU0 2# t1 FWD DETAIL:415: l2tp session
table rebuilt
   Jul 27 14:39:52.106 l2vpn/issu 0/RSP0/CPU0 1# t1 ISSU:788: ISSU - iMDR init called;
'infra/imdr' detected the 'informational' condition 'the service is not supported in the
   Jul 27 14:39:52.107 12vpn/issu 0/RSP0/CPU0 1# t1 ISSU:428: ISSU - attempt to start
COLLABORATOR wait timer while not in ISSU mode
   Jul 27 14:39:54.286 12vpn/fwd-common 0/RSP0/CPU0 1# t1 FWD COMMON:3257: show edm thread
 initialized
   Jul 27 14:39:55.270 l2vpn/fwd-mac 0/RSP0/CPU0 1# t1 FWD MAC|ERR:783: Mac aging init
   Jul 27 14:39:55.286 l2vpn/fwd-mac 0/RSP0/CPU0 1# t1 FWD MAC:1765: l2vpn gsp cons init
 returned No error
    Jul 27 14:39:55.340 12vpn/fwd-mac 0/RSP0/CPU0 1# t1 FWD MAC:1792: Client successfully
 joined gsp group
   Jul 27 14:39:55.340 12vpn/fwd-mac 0/RSP0/CPU0 1# t1 FWD MAC:779: Initializing the
txlist IPC thread
   Jul 27 14:39:55.341 l2vpn/fwd-mac 0/RSP0/CPU0 1# t1 FWD_MAC:2971: gsp_optimal_msg_size
 = 4832 (real: True)
   Jul 27 14:39:55.351 12vpn/fwd-mac 0/RSP0/CPU0 1# t1 FWD MAC:626: Entering mac aging
timer init
```

# show I2vpn xconnect

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

show | 12vpn | xconnect | [{brief | detail | encapsulation | group | groups | interface | location | mp2mp | mspw | neighbor | pw-class | standby | state | summary | type | state | unresolved | pw-id | value}]

## **Syntax Description**

brief	(Optional) Displays encapsulation brief information.
detail	(Optional) Displays detailed information.
encapsulation	(Optional) Filters on encapsulation type.
group	(Optional) Displays all cross-connects in a specified group.
groups	(Optional) Displays all groups information.
interface	(Optional) Filters the interface and subinterface.
location	(Optional) Displays location specific information.
mp2mp	(Optional) Displays MP2MP information.
mspw	(Optional) Displays ms_pw information.
neighbor	(Optional) Filters the neighbor.
pw-class	(Optional) Filters on pseudowire class
standby	(Optional) Displays standby node specific information.
state	(Optional) Filters the following xconnect state types:
	• up
	• down
summary	(Optional) Displays AC information from the AC Manager database.
type	(Optional) Filters the following xconnect types:
	• ac-pw
	• locally switched
state unresolved	(Optional) Displays information about unresolved cross-connects.
pw-id value	Displays the filter for 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 3.4.1 VCCV-related show command output was added.

Release 3.6.0 Preferred-path-related show command output was added.

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

Release 4.3.0 The following keywords were introduced:

- brief
- · encapsulation
- · groups
- · location
- mp2mp
- mspw
- pw-class
- standby

Release 5.1.2 This command was modified to enable filtering the command output for a specific pseudowire with just the pseudowire ID.

## **Usage Guidelines**

To use this command, you must be in a user group associated with a task 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.

When configuring Ethernet Connectivity Fault Managment (CFM) over l2vpn cross-connect, the CFM Continuity Check Messages (CCM) packets are not accounted for in the cross-connect pseudowire packet counters displayed in this show command output.



Note

For Cisco IOS XR software Release 5.1.2 and above, you can filter the command output for specific pseudowire with just the pseudowire ID. However, for pseudowire configurations with FEC 129 Type 2 (in VPWS), filtering the output for a specific pseudowire can only be done with the combination of the neighbour filter and the pseudowire ID.

#### Task ID

Task Operations ID 

12vpn read, write

#### **Examples**

The following example shows sample output for the show 12vpn xconnect command:

```
RP/0/RP0/CPU0:router# show 12vpn xconnect
Wed May 21 09:06:47.944 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
      SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
XConnect
                       Segment 1
                                                  Segment 2
       Name ST Description
Group
                                          ST
                                                 Description
                                                                     ST
L2TPV3 V4 XC GRP
        L2TPV3 P2P 1
               UP Gi0/2/0/1.2 UP 26.26.26.26 100 UP
L2TPV3 V4 XC GRP
         L2TPV3 P2P 2
                  UP Gi0/2/0/1.3
                                          UP
                                                 26.26.26.26
                                                                200 UP
```

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

```
RP/0/RP0/CPU0:router# show 12vpn 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
    ______ ____
   Label
              30005
   Group ID 0x5000300
Interface GigabitEthernet0/4/0/1 GigabitEthernet0/4/0/1
GigabitEthernet0/3/0/1
                                           GigabitEthernet0/4/0/2
   MTII
                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
     30006
     Label
                                              16003
     Group ID unassigned Interface unknown MTU 1500
                                              0x5000400
                                               GigabitEthernet0/4/0/2
                                              1500
     Control word enabled
                                              enabled
     PW type Ethernet
                                             Ethernet
     VCCV CV type 0x2
                                              0x2
                                             (LSP ping verification) 0x3
                 (LSP ping verification)
     VCCV CC type 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 12vpn xconnect
 detail command:
RP/0/RP0/CPU0:router# show 12vpn 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
                 30005
                                              unknown
     Group ID 0x5000300
                                               0 \times 0
     Interface GigabitEthernet0/4/0/1
                                             unknown
      Interface
                                                  GigabitEthernet0/3/0/1
                  pw-span-test
     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
Group ID unassigned
                                              16003
                                              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 12vpn 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/RP0/CPU0:router# show 12vpn 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
        Name ST Description
Group
                                            ST Description
siva xc siva p2p UP Gi0/4/0/1
                                            UP 1.1.1.1 1 UP
                                                  Backup
                                                  2.2.2.2
______
The following sample output shows that the backup is in standby mode for the show l2vpn
 xconnect detail command:
RP/0/RP0/CPU0:router# show 12vpn 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
      MPT<sub>i</sub>S
                 Local
                                               Remot.e
```

```
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)
     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
                                                Remot.e
     Label 30006
                                              16003
     Group ID unassigned
                                              0×5000400
     Interface unknown
                                              GigabitEthernet0/4/0/2
     MTU
                1500
                                              1500
                                              enabled
     Control word enabled
     PW type Ethernet
                                              Ethernet
     VCCV CV type 0x2
                                              0 \times 2
                 (LSP ping verification)
                                             (LSP ping verification)
     VCCV CC type 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 12vpn xconnect
 detail command:
RP/0/RP0/CPU0:router# show 12vpn 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
   Group ID 0x5000300
                                           0 \times 0
   Interface GigabitEthernet0/4/0/1
                                           unknown
               1500
                                           unknown
   Control word enabled
                                           unknown
   PW type Ethernet
                                           unknown
   VCCV CV type 0x2
                                           0 \times 0
                                           (none)
               (LSP ping verification)
   VCCV CC type 0x3
                                          0 \times 0
                                           (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
Group ID unassigned
                                           16003
                                           0×5000400
   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/RP0/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
                0x120001c0
     Group ID
                                                0x120001c0
     Interface GigabitEthernet0/7/0/5.3
                                                GigabitEthernet0/7/0/5.3
                  1508
                                                1508
     Control word disabled
                                                disabled
     PW type Ethernet
                                               Ethernet
     VCCV CV type 0x2
                                               0x2
                 (LSP ping verification)
                                               (LSP ping verification)
     VCCV CC type 0x6
                                                0x6
                  (router alert label)
                                                (router alert label)
                                                (TTL expiry)
                  (TTL expiry)
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 4294705365
Create time: 21/09/2011 08:05:01 (00:14:01 ago)
Last time status changed: 21/09/2011 08:07:01 (00:12:01 ago)
Statistics:
packets: received 1336, sent 26392092
bytes: received 297928, sent 1583525520
```

This example shows the sample output of a pseudowire headend (PWHE) cross connect:

```
RP/0/RP0/CPU0:router# show l2vpn xconnect interface pw-ether 67 detail
Group gl, XC xcl, state is down; Interworking none
 AC:PW-Ether1, state is up
   Type PW-Ether
    Interface-list: interfacelist1
   Replicate status:
     Gi0/2/0/1: success
     Gi0/3/0/1: pending
     Gi0/4/0/1: failed
   MTU 1500; interworking none
   Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  PW: neighbor 130.130.130.130, PW ID 1234, state is down (provisioned)
   PW class not set
    Encapsulation MPLS, protocol LDP
   PW type Ethernet VLAN, control word disabled, interworking none
   Sequencing not set
   Internal label: 16008
   VLAN id imposed: 101
     _____
                                               unknown
```

```
Group ID
              0x2000600
             PW-Ether1
  Interface
                                     unknown
  MTU
              1500
                                              unknown
  Control word disabled
                                             unknown
  PW type Ethernet VLAN
                                             unknown
  VCCV CV type 0x2
                                              0x0
                                              (none)
               (LSP ping verification)
  VCCV CC type 0x6
                                              0x0
                                              (none)
               (router alert label)
               (TTL expiry)
MIB cpwVcIndex: 2
Create time: 19/02/2010 23:13:01 (1w2d ago)
Last time status changed: 19/02/2010 23:13:16 (1w2d ago)
Statistics:
  packets: received 0, sent 0
  bytes: received 0, sent 0
```

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

```
RP/0/RP0/CPU0:router# show l2vpn xconnect detail

Group g1, XC p1, state is up; Interworking none

AC: GigabitEthernet0/0/1/1, state is up

Type Ethernet

MTU 1500; XC ID 0x1000002; interworking none

Statistics:

packets: received 24688, sent 24686

bytes: received 1488097, sent 1487926

PW: neighbor 3.3.3.3, PW ID 2, state is up ( established )

PW class class1, XC ID 0x1000002

Encapsulation MPLS, protocol LDP

PW type Ethernet, control word disabled, interworking none

PW backup disable delay 0 sec

Sequencing not set

Flow label flags configured (Rx=1,Tx=1), negotiated (Rx=0,Tx=1)
```

This table describes the significant fields shown in the display.

#### Table 8: show I2vpn 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).

Command	Description
xconnect group, on page 138	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	Hace	PIN	1110	
JVIIIAX	レじるし	110	uu	ш

*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

### Example

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

```
RP/0/RP0/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
                14213298 pkts 1250770344 bytes
Transmit:
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/RP0/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 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

Command	Description
tunnel-template, on page 137	Enters tunnel-template configuration submode.

## storm-control

Storm control on ASR 9000 Series Routers can be applied at the following service attachment points:

- Bridge domain (BD)
- Attachment Circuit (AC)
- Access pseudowire (PW)

To enable storm control on all access circuits (AC) and access pseudowires (PW) in a VPLS bridge, use the **storm-control** command in l2vpn bridge group bridge-domain configuration mode. To disable storm control, use the **no** form of this command.

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

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

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

## **Syntax Description**

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

#### **Command Default**

Storm control is disabled by default.

## **Command Modes**

12vpn bridge group bridge-domain access circuit configuration

## **Command History**

Release	Modification
Release 3.7.2	This command was introduced.

## **Usage Guidelines**

- Bridge Protocol Data Unit (BPDU) packets are not filtered through the storm control feature.
- The traffic storm control monitoring interval is set in the hardware and is not configurable. On Cisco ASR 9000 Series Router, the monitoring interval is always one second.
- When there is a mix of kbps and pps storm control on bridge or bridge port, the pps value is translated to kbps inside the policer using 1000 bytes per packet as an average.
- The hardware can only be programmed with a granularity of 8 pps, so values are not divisible by eight. These are rounded to the nearest increment of eight.

#### Task ID

Task ID	Operations
12vpn	read, write

## **Examples**

The following example enables storm control thresholds throughout the bridge domain:

```
RP/0/RSP0/CPU0:a9k1# configure
RP/0/RSP0/CPU0:a9k1(config) # 12vpn
RP/0/RSP0/CPU0:a9k1(config-12vpn) # bridge group BG1
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg) # bridge-domain BD1
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd) # storm-control unknown-unicast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd) # storm-control multicast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd) # storm-control broadcast pps 100
```

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

```
RP/0/RSP0/CPU0:a9k1# configure
RP/0/RSP0/CPU0:a9k1(config)# 12vpn
RP/0/RSP0/CPU0:a9k1(config-12vpn)# bridge group BG1
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd)# bridge-domain BD2
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd)# interface Bundle-Ether9001.2001
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-ac)# storm-control unknown-unicast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-ac)# storm-control multicast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-ac)# storm-control broadcast pps 100
```

The following example enables storm control thresholds on an access pseudowire:

```
RP/0/RSP0/CPU0:a9k1# configure
RP/0/RSP0/CPU0:a9k1(config)# 12vpn
RP/0/RSP0/CPU0:a9k1(config-12vpn)# bridge group BG1
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd)# bridge-domain BD2
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-ac)# neighbor 10.1.1.1 pw-id 20011001
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-pw)# storm-control unknown-unicast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-pw)# storm-control multicast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-pw)# storm-control broadcast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-pw)# commit
```

### **Running Configuration**

```
12vpn
bridge group BG1
bridge-domain BD1
storm-control unknown-unicast pps 100
```

```
storm-control multicast pps 100
  storm-control broadcast pps 100
 bridge-domain BD2
  interface Bundle-Ether9001.2001
   storm-control unknown-unicast pps 100
   storm-control multicast pps 100
   storm-control broadcast pps 100
  neighbor 10.1.1.1 pw-id 20011001
   storm-control unknown-unicast pps 100
   storm-control multicast pps 100
   storm-control broadcast pps 100
  !
 !
 !
end
RP/0/RSP0/CPU0:a9k1(config)#
```

## tag-impose

To specify a tag for a VLAN ID configuration, use the **tag-impose** command in l2vpn configuration submode. To remove the tag, use the **no** form of this command.

tag-impose vlan value no tag-impose vlan value

## **Syntax Description**

vlan	VLAN in tagged mode.
value	Tag value. The range is from 1 to 4094. The default value is 0.

## **Command Default**

None

### **Command Modes**

L2VPN configuration

## **Command History**

Release	Modification
Release 4.2.1	This command was introduced.

## **Usage Guidelines**

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

### Task ID

Task ID	Operations
l2vpn	read, write

## **Examples**

This example shows how to specify a tag for a VLAN:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-l2vpn)# xconnect group xc1
RP/0/RP0/CPU0:router(config-l2vpn-xc)#p2p grp1
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p)#neighbor 10.1.1.2 pw-id 78
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p-pw)#tag-impose vlan 8
```

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

## 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 3.6.0	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# pw-class kanata01
RP/0/RP0/CPU0:router(config-12vpn-pwc)# encapsulation mpls
RP/0/RP0/CPU0:router(config-12vpn-pwc-encap-mpls)# tag-rewrite vlan 2000
RP/0/RP0/CPU0:router(config-12vpn-pwc-encap-mpls)#

Command	Description
show I2vpn xconnect, on page 116	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 3.9.0	This command was introduced.

## **Usage Guidelines**

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

#### Task ID

Task ID	Operations
12vpn	read, write

## **Examples**

The following example shows how to configure a timeout value for L2TP session setup of 400 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12tp-class cisco
RP/0/RP0/CPU0:router(config-l2tp-class)# timeout setup 400
```

Command	Description
authentication (L2TP), on page 11	Enables L2TP authentication for a specified L2TP class name.
hello-interval (L2TP), on page 28	Configures the hello-interval value for L2TP (duration between control channel hello packets).
hidden (L2TP), on page 30	Enables hidden attribute-value pairs (AVPs).
hostname (L2TP), on page 32	Defines the name used in the L2TP hostname AVP.
l2tp-class, on page 36	Enters L2TP class configuration mode where you can define an L2TP signaling template.

Command	Description	
password (L2TP), on page 55	Defines the password and password encryption type for control channel authentication.	
receive-window (L2TP), on page 66	Configures the receive window size for the L2TP server.	
retransmit (L2TP), on page 68	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 disable the L@VPN pseudowire class transport mode configuration, 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
12vpn	read, write

# Examples

This example shows how to configure Ethernet transport mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# pw-class kanata01
RP/0/RP0/CPU0:router(config-12vpn-pw)# encapsulation mpls
RP/0/RP0/CPU0:router(config-12vpn-encap-mpls)# transport-mode ethernet
```

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

# transport mode vlan passthrough

To configure L2VPN bridge domain transport mode, use the **transport mode vlan passthrough** command in L2VPN bridge domain configuration mode. To disable the L2VPN bridge domain transport mode configuration, use the **no** form of this command.

transport mode vlan passthrough no transport mode vlan passthrough

**Syntax Description** 

This command has no keywords or arguments.

**Command Default** 

None

**Command Modes** 

L2VPN bridge domain configuration

**Command History** 

Release	Modification
Release 4.3.1	This command was introduced.

#### **Usage Guidelines**

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



Note

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

# Task ID

Task ID	Operations
l2vpn	read, write

# **Examples**

This example shows how to configure transport mode vlan passthrough:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group bg1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bd1
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# transport mode vlan passthrough
```

Command	Description	
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.	

# 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# tunnel-template template\_01

Command	Description
xconnect group, on page 138	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-l2vpn)# xconnect group customer\_atlantic

Command	Description
show l2vpn xconnect, on page 116	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), on page 140
- aging (VPLS), on page 142
- bridge-domain (VPLS), on page 144
- bridge group (VPLS), on page 145
- clear 12vpn bridge-domain (VPLS), on page 146
- flooding disable, on page 147
- interface (VPLS), on page 149
- learning disable (VPLS), on page 151
- limit (VPLS), on page 153
- mac (VPLS), on page 155
- maximum (VPLS), on page 157
- mpls static label (VPLS), on page 159
- mtu (VPLS), on page 161
- neighbor (VPLS), on page 163
- notification (VPLS), on page 165
- port-down flush disable (VPLS), on page 167
- pw-class (VFI), on page 169
- show 12vpn bridge-domain (VPLS), on page 171
- show 12vpn forwarding bridge-domain (VPLS), on page 180
- show 12vpn forwarding bridge-domain mac-address (VPLS), on page 196
- shutdown (Bridge Domain), on page 207
- shutdown (VFI), on page 208
- static-address (VPLS), on page 210
- static-mac-address (VPLS), on page 212
- time (VPLS), on page 214
- type (VPLS), on page 216
- vfi (VPLS), on page 218
- withdraw (VPLS), on page 220

# 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**

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 3.8.0	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 **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
12vpn	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/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config) #12vpn
RP/0/RP0/CPU0:router(config-l2vpn) #bridge group 1

```
RP/0/RP0/CPU0:router(config-12vpn-bg) #bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd) #mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac) #limit
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac-limit) #action flood
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac-limit) #maximum 10
```

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	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 153	Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
I2vpn, on page 44	Enters L2VPN configuration mode.
mac (VPLS), on page 155	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 157	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 165	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 214 and the type (VPLS), on page 216 parameters.

## **Command Modes**

L2VPN bridge group bridge domain MAC 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 **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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac)# aging
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac-aging)# time 120
```

Commands	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.

Commands	Description
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then assigns network interfaces to the bridge domain.
12vpn, on page 44	Enters L2VPN configuration mode.
mac (VPLS), on page 155	Enters L2VPN bridge group bridge domain MAC configuration mode.
time (VPLS), on page 214	Configures the maximum aging time.
type (VPLS), on page 216	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 3.8.0	This command was introduced	

# **Usage Guidelines**

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

## Task ID

Task ID	Operations
l2vpn	read, write

## **Examples**

The following example shows how to configure a bridge domain:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)#

Command	Description
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	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 3.8.0	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 **bridge group** command to enter L2VPN bridge group configuration mode.

# Task ID

Task ID	Operations
12vpn	read, write

## **Examples**

The following example shows that bridge group 1 is assigned:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)#

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
l2vpn, on page 44	Enters L2VPN configuration mode.

# clear I2vpn bridge-domain (VPLS)

To clear the MAC addresses and to restart the bridge domains on the router, use the **clear 12vpn bridge-domain** command in EXEC mode.

clear 12vpn 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 <i>name</i> 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 3.8.0	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.

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/RP0/CPU0:router# clear 12vpn bridge-domain all

Command	Description
show I2vpn bridge-domain (VPLS), on page 171	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 3.8.0	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 **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
12vpn	read, write

# Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# flooding disable
```

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
mtu (VPLS), on page 161	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 3.8.0	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 **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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
```

RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/9
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ac)#

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	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 3.8.0	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.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)# learning disable
```

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
mac (VPLS), on page 155	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 3.8.0	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 **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
12vpn	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac)# limit
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac-limit)# maximum 100
```

RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac-limit)# action shutdown
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac-limit)# notification both

Description
Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
Enters L2VPN configuration mode.
Enters L2VPN bridge group bridge domain MAC configuration mode.
Configures the specified action when the number of MAC addresses learned on a bridge is reached.
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 3.8.0	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 mac command to enter L2VPN bridge group bridge domain MAC configuration mode.

# Task ID

Task ID	Operations
12vpn	read, write

# **Examples**

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac)#
```

Command	Description
aging (VPLS), on page 142	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
learning disable (VPLS), on page 151	Overrides the MAC learning configuration of a parent bridge or sets the MAC learning configuration of a bridge.
limit (VPLS), on page 153	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 210	Adds static entries to the MAC address for filtering.
withdraw (VPLS), on page 220	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 3.8.0 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.

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
12vpn	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac)# limit

RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# maximum 5000
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# action no-flood

Description
Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
Enters L2VPN configuration mode.
Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
Enters L2VPN bridge group bridge domain MAC configuration mode.
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

Configures the remote pseudowire label.

value 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 3.8.0	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.

Ensure that both ends of the pseudowire have matching static labels.

## Task ID

Task ID	Operations
12vpn	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# vfi model
```

RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# mpls static label local 800 remote 500

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
neighbor (VPLS), on page 163	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
pw-class (VFI), on page 169	Configures the pseudowire class template name to use for the pseudowire.
vfi (VPLS), on page 218	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 3.8.0	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.

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
12vpn	read, write

## **Examples**

The following example specifies an MTU of 1000 bytes:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group 1
```

RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# mtu 1000

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	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 147	Configures flooding for traffic at the bridge domain level or at the bridge port level.
I2vpn, on page 44	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.
<b>pw-id</b> 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 3.8.0	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 **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
12vpn	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# vfi v1
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-vfi-pw)#
```

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 159	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
pw-class (VFI), on page 169	Configures the pseudowire class template name to use for the pseudowire.
static-mac-address (VPLS), on page 212	Configures the static MAC address to associate a remote MAC address with a pseudowire or any other bridge interface.
vfi (VPLS), on page 218	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 3.8.0	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.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
```

RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)# limit
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# notification both

Description
Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
Enters L2VPN configuration mode.
Enters L2VPN bridge group bridge domain MAC configuration mode.
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
12vpn	read, write

# **Examples**

The following example shows how to disable MAC flush when the bridge port is nonfunctional:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac)# port-down flush disable
```

Command	Description
action (VPLS), on page 140	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
mac (VPLS), on page 155	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 157	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 165	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 3.8.0	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
12vpn	read, write

## **Examples**

The following example shows how to attach the pseudowire class to the pseudowire:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# pw-class canada
```

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.

Command	Description
I2vpn, on page 44	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 159	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 163	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
vfi (VPLS), on page 218	Configures virtual forwarding interface (VFI) parameters.

# show I2vpn 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 12vpn bridge-domain [{bd-name bridge-domain-name | brief | detail | group
bridge-domain-group-name | interface type interface-path-id | pw-id value }] neighbor IP-address
[{pw-id value | summary}]

### **Syntax Description**

bd-name	(Optional) Displays the bridges by the bridge ID. The bridge-domain-name	
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.	
<b>group</b> bridge-domain-group-name	(Optional) Displays filter information on the bridge-domain group name. The <i>bridge-domain-group-name</i> 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.	
	<b>Note</b> Use the <b>show interfaces</b> 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 <i>IP-address</i> 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 mode

## **Command History**

Release	Modification
Release 3.8.0	This command was introduced.

Release	Modification
Release 5.1.2	This command was modified to enable filtering the command output for specific pseudowire with just the pseudowire ID.

### **Usage Guidelines**

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any 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.



Note

For Cisco IOS XR software Release 5.1.2 and above, you can filter the command output for a specific pseudowire with just the pseudowire ID. However, in case of configurations with BGP Auto-discovery with BGP or LDP signaling (in VPLS), you can specify the pseudowire only with the combination of the neighbor filter and the pseudowire ID.

#### Task ID

Task ID	Operations
12vpn	read

#### **Examples**

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

```
RP/0/RP0/CPU0:router# show l2vpn bridge-domain bd-name bg1 bd1 detail
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: bg1 bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  Coupled state: disabled
  MAC learning: enabled
  MAC withdraw: enabled
   MAC withdraw for Access PW: enabled
   MAC withdraw sent on: bridge port up
   MAC withdraw relaying (access to access): disabled
  Flooding:
   Broadcast & Multicast: enabled
   Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: no
  MAC port down flush: enabled
  MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
  Dynamic ARP Inspection: disabled, Logging: disabled
  IP Source Guard: disabled, Logging: disabled
  DHCPv4 snooping: disabled
  IGMP Snooping: enabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
```

```
Storm Control: disabled
Bridge MTU: 1500
MIB cvplsConfigIndex: 1
Filter MAC addresses:
P2MP PW: disabled
Create time: 30/03/2015 22:25:38 (00:26:08 ago)
No status change since creation
ACs: 2 (2 up), VFIs: 1, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
 AC: BVI1, state is up
   Type Routed-Interface
   MTU 1514; XC ID 0x80000001; interworking none
   BVI MAC address:
     1000.4444.0001
  AC: GigabitEthernet0/8/0/0.1, state is up
    Type VLAN; Num Ranges: 1
    Outer Tag: 1
    VLAN ranges: [1001, 1001]
   MTU 1508; XC ID 0x508000a; interworking none
   MAC learning: enabled
   Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
   MAC aging time: 300 s, Type: inactivity
   MAC limit: 4000, Action: none, Notification: syslog
   MAC limit reached: no
   MAC port down flush: enabled
   MAC Secure: disabled, Logging: disabled
    Split Horizon Group: none
   Dynamic ARP Inspection: disabled, Logging: disabled
   IP Source Guard: disabled, Logging: disabled
   DHCPv4 snooping: disabled
    IGMP Snooping: enabled
    IGMP Snooping profile: none
   MLD Snooping profile: none
   Storm Control: bridge-domain policer
   Static MAC addresses:
   Storm control drop counters:
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0
    Dynamic ARP inspection drop counters:
     packets: 0, bytes: 0
    IP source guard drop counters:
     packets: 0, bytes: 0
List of VNIs:
  VNI 1, state is up
   XC ID 0x80000014
   Encap type VXLAN
    Overlay nve100, Source 1.1.1.1, Multicast Group 225.1.1.1, UDP Port 4789
    Anycast VTEP 100.1.1.1, Anycast Multicast Group 224.10.10.1
   MAC learning: enabled
   Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
   MAC aging time: 300 s, Type: inactivity
   MAC limit: 4000, Action: none, Notification: syslog
   MAC limit reached: no
   MAC port down flush: enabled
   MAC Secure: disabled, Logging: disabled
    Split Horizon Group: none
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    DHCPv4 snooping: disabled
```

```
IGMP Snooping: enabled
IGMP Snooping profile: none
MLD Snooping profile: none
Storm Control: bridge-domain policer

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

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/RP0/CPU0:router# show 12vpn 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 I2vpn 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/RP0/CPU0:router# show 12vpn 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:

q1/bd1

1/1

```
RP/0/RP0/CPU0:router# show 12vpn bridge-domain brief

Bridge Group/Bridge-Domain Name ID State Num ACs/up Num PWs/up
```

up

0

This table describes the significant fields shown in the display.

#### Table 10: show I2vpn 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.

1/1

The following sample output shows detailed information:

```
RP/0/RP0/CPU0:router# show 12vpn 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
                                                        Remote
       Label 16003
                                                16003
                   0x0
                                                  0x0
       Group ID
       Interface 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/RP0/CPU0:router# show 12vpn bridge-domain detail
```

```
Bridge group: foo_group, bridge-domain: foo bd, id: 0, state: up, ShqId: 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 VFTs:
   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
   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
              Local
   Label
            16002
                                         16002
   Group ID unassigned
   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) (router alert label)
            (control word)
                                         (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 I2vpn 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/RP0/CPU0:router# show 12vpn 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

```
RP/0/RP0/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/RP0/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/RP0/CPU0:router# show 12vpn 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 example shows the sample output of a configured flow label:

```
RP/0/RP0/CPU0:router# show 12vpn bridge-domain detail
Bridge group: g1, bridge-domain: d1, id: 0, state: up, ShgId: 0, MSTi: 0
.....
PW: neighbor 3.3.3.3, PW ID 2, state is up ( established )
   PW class class1, XC ID 0x1000002
   Encapsulation MPLS, protocol LDP
   PW type Ethernet, control word disabled, interworking none
   PW backup disable delay 0 sec
Sequencing not set
   Flow label flags configured (Rx=1,Tx=1), negotiated (Rx=0,Tx=1)
```

This table describes the significant fields shown in the display.

### Table 12: show I2vpn 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 146	Clears the MAC addresses and restarts the bridge domains on the router.

## show I2vpn 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 <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

### **Command Default**

None

## **Command Modes**

**EXEC** 

## **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.

For each bridge, you can display summary information about the number of bridge ports, number of MAC addresses, configured VXLANs 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/RP0/CPU0:router# show 12vpn forwarding bridge-domain location 0/1/CPU0
                                ID
                                      Ports addr Flooding Learning State
Bridge-Domain Name
_____
al: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/RP0/CPU0:router
Bridge-domain name: gl:bdl, 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 ]
[ 0x0000000 00000000 00000000 00000000 ]
       SHG-TX encap details
______
                       0
outer_etype:
                        0
outer vlan id:
gather profile:
                        0
inner vlan id:
so 12 len adjust:
       SHG-TX mgid details
       Base MGIDs for default mgid
base mgid[0]:
                   0x0003fffb
base mgid[1]:
                   0x0003fffb
                   0x0003fffb
base_mgid[2]:
base mgid[3]:
                   0x0003fffb
                   0x0003fffb
base mgid[4]:
base mgid[5]:
                   0x0003fffb
base mgid[6]:
                   0x0003fffb
base_mgid[7]:
                   0x0003fffb
     MGID Entries for default mgid
     0
16384
oi[0]:
oq[0]:
xc id[0]:
             1
VMR 0 Details
vmrid: 0x5f002010
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
12fwd enabled:
                       true
plim enabled:
                        true
12fwd type:
12 ac type:
                        0
xconn id:
```

```
bridge id:
shg id:
unicast flooding enabled:
                              0
multicast flooding enabled: 0
                             0
broadcast flooding enabled:
mac learning enabled:
                              0
Is AC Port mode?:
                          0
HW Rewrite O 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
[ 0x00000000 0036062c 0003fffc 00000000 ]
[ 0x00000000 00000000 0d103600 00000010 ]
[ 0x00000000 00000000 00000000 00000000 ]
BP OI/OQ Details

      oi[0]:
      0x00000000
      oq[0]

      oi[1]:
      0x0000000
      oq[1]

      oi[2]:
      0x0000000
      oq[2]

      oi[3]:
      0x00000000
      oq[3]

                                                16384
                                                65535
                                               65535
                                              65535
            0x0000000
                                              65535
oi[4]:
                             oq[4]
                              oq[5]
            0x0000000
0x00000000
                                               65535
oi[5]:
oi[6]:
                               oq[6]
                                                65535
             0x00000000
oi[7]:
                                                65535
                               oq[7]
 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
oi[1]: 0x00000000
                          oq[0]
                                                65535
                               oq[1]
                                                65535
             0x0000000
                              oq[2]
oi[2]:
                                               65535
oi[3]:
            0x00000000
                              oq[3]
                                               65535
oi[4]:
            0x0000000
                              oq[4]
                                               65535
            0x00000000
oi[5]:
                              oq[5]
                                               65535
                              oq[6]
oi[6]:
              0x00000000
             0x0000000
                              oq[7]
                                                65535
BP Encap Info
_____
mac_length: 0
mac string:
egress_slot: 2
num tags:
```

```
tags: {16001, }
if_handle: 0x03000500
```

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

```
RP/0/RP0/CPU0:router# show 12vpn forwarding bridge-domain g1:bd1 location 0/1/CPU0
```

The following sample output shows the hardware information for a specific bridge-domain:

```
RP/0/RP0/CPU0:router#show 12vpn bridge-domain hardware
```

```
Bridge group: aa, bridge-domain name: g1, id:0
FGID Boardcast [version 1]:
Allocate_count: 2048, Retry_count: 0, Realloc_on: Off
Status_flag: (0x4) Replay-end
ALL 44032, VFI 44033

Bridge group: aa, bridge-domain name: g2, id:1
FGID Boardcast [version 1]:
Allocate_count: 2048, Retry_count: 0, Realloc_on: Off
Status_flag: (0x4) Replay-end
ALL 44034, VFI 44035
```

The following sample output shows the hardware information for the line card, for a specific bridge-domain on the ingress detail location:

#### RP/0/RP0/CPU0:router#

#### show 12vpn forwarding bridge-domain hardware ingress detail location 0/2/CPU0

```
Bridge-domain name: aa:g1, 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
Bridge MTU: 1500 bytes
Number of bridge ports: 4
 Number of MAC addresses: 0
Multi-spanning tree instance: 0
  INGRESS BRIDGE [version, state]: [1, CREATED]
        TCAM entry seg#: 1024 Key: [BID: 0 MAC: default]
        HW: 0x4c000000 0x000080ac 0x00010000 0x80ac0100
        SW: 0x4c000000 0x000080ac 0x00010000 0x80ac0100
        SMAC: action: PUNT state: NO REFRESH
        DMAC: action: FLOOD, flood enable: enable
        FGID: All: 44032, VFI: 44033, MCAST Sponge q: 16
        Fabric multicast1: 1 Fabric multicast2: 1
        Admin State: UP
        MTU: 1500
```

```
Number of MAC addresses: 1 (0 MAC + 1 default)
     ACL NAME (ACL-ID): VPLS Special (4096)
     TCAM region handle : 5
GigabitEthernet0/2/0/1.1, state: oper up
 Number of MAC: 0
 Statistics:
   packets: received 0, sent 0
   bytes: received 0, sent 0
INGRESS BRIDGE PORT [version, state]: [1, BOUND]
     Bridge Port Type: AC
     XID: 0/2/CPU0 : 1 (0x1280001)
     Bridge ID: 0, Split Horizon ID: 0
     RX TLU1 : 0x4c00
              : 0x1013c00
     RX TLU2
               : 0x200ba00
     RX TLU3
     RX TLU4 : 0x3000c00
INGRESS AC [version, state]: [1, BOUND]
     Xconnect-ID: [1] TCAM-Key: (UIDB:0x2 O-vlan:1 I-vlan:0 Ether-Type:0x8100)
     HW: 0x24001000 0x01280001 0x10128000 0xc7ff7d00
     SW: 0x24001000 0x01280001 0x10128000 0xc7ff7d00
     Service type: 4 (bridging pmp)
     Entry type: 1 (fwd)
     Bridge ID : 0
     ACL_ID : 4096
     Xconnect ID : 0x1280001
     SplitHorizonGroup ID: 0
     Rewrite supported: 0 (No)
     PW mode: 0 (vc-type 5)
     AC-type: 1 (vlan-mode)
     Interface handle: 0x128000
     Ingress AC stats: 0x7ff7d
     SMAC Learning: enable
     DMAC Flooding: enable
GigabitEthernet0/2/0/1.2, state: oper up
 Number of MAC: 0
  Statistics:
   packets: received 0, sent 0
   bytes: received 0, sent 0
INGRESS BRIDGE PORT [version, state]: [1, BOUND]
     Bridge Port Type: AC
     XID: 0/2/CPU0 : 2 (0x1280002)
     Bridge ID: 0, Split Horizon ID: 0
     RX TLU1 : 0x4c01
     RX TLU2 : 0x1013c01
     RX TLU3 : 0x200ba01
     RX TLU4 : 0x3000c01
INGRESS AC [version, state]: [1, BOUND]
     Xconnect-ID: [2] TCAM-Key: (UIDB:0x2 O-vlan:2 I-vlan:0 Ether-Type:0x8100)
     HW: 0x24001000 0x01280002 0x10128002 0xc7ff7a00
     SW: 0x24001000 0x01280002 0x10128002 0xc7ff7a00
     Service type: 4 (bridging pmp)
     Entry type: 1 (fwd)
```

```
Bridge ID: 0
        ACL ID : 4096
        Xconnect ID : 0x1280002
        SplitHorizonGroup ID: 0
       Rewrite supported: 0 (No)
        PW mode: 0 (vc-type 5)
        AC-type: 1 (vlan-mode)
        Interface handle: 0x128002
        Ingress AC stats: 0x7ff7a
        SMAC Learning: enable
        DMAC Flooding: enable
  GigabitEthernet0/2/0/1.3, state: oper up
   Number of MAC: 0
   Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  INGRESS BRIDGE PORT [version, state]: [1, BOUND]
       Bridge Port Type: AC
       XID: 0/2/CPU0 : 3 (0x1280003)
       Bridge ID: 0, Split Horizon ID: 0
       RX TLU1 : 0x4c02
       RX TLU2
                : 0x1013c02
       RX TLU3 : 0x200ba02
       RX TLU4 : 0x3000c02
   INGRESS AC [version, state]: [1, BOUND]
        Xconnect-ID: [3] TCAM-Key: (UIDB:0x2 O-vlan:3 I-vlan:0 Ether-Type:0x8100)
        HW: 0x24001000 0x01280003 0x10128004 0xc7ff7700
        SW: 0x24001000 0x01280003 0x10128004 0xc7ff7700
       Service type: 4 (bridging pmp)
       Entry type: 1 (fwd)
        Bridge ID : 0
       ACL ID : 4096
        Xconnect_ID : 0x1280003
        SplitHorizonGroup ID: 0
       Rewrite supported: 0 (No)
        PW mode: 0 (vc-type 5)
       AC-type: 1 (vlan-mode)
        Interface handle: 0x128004
        Ingress AC stats: 0x7ff77
        SMAC Learning: enable
        DMAC Flooding: enable
 Nbor 5.0.0.5 pw-id 1
   Number of MAC: 0
   Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  INGRESS BRIDGE PORT [version, state]: [1, BOUND]
       Bridge Port Type: ATOM
       XID: 127/15/CPU0 : 1 (0xfff80001)
       Bridge ID: 0, Split Horizon ID: 1
        VC label: 16006
        Control-word supported: No
Bridge-domain name: aa:g2, id: 1, 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
Bridge MTU: 1500 bytes
Number of bridge ports: 2
Number of MAC addresses: 0
Multi-spanning tree instance: 0
 INGRESS BRIDGE [version, state]: [1, CREATED]
       TCAM entry seq#: 1025 Key: [BID: 1 MAC: default]
       HW: 0x4c000000 0x000080ac 0x02010000 0x80ac0300
       SW: 0x4c000000 0x000080ac 0x02010000 0x80ac0300
       SMAC: action: PUNT state: NO REFRESH
       DMAC: action: FLOOD, flood_enable: enable
       FGID: All: 44034, VFI: 44035, MCAST Sponge q: 16
       Fabric multicast1: 1 Fabric multicast2: 1
       Admin State: UP
       MTU: 1500
       Number of MAC addresses: 1 (0 MAC + 1 default)
       ACL NAME (ACL-ID): VPLS Special (4097)
       TCAM region handle : 5
 GigabitEthernet0/2/0/1.4, state: oper up
   Number of MAC: 0
   Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
 INGRESS BRIDGE PORT [version, state]: [1, BOUND]
       Bridge Port Type: AC
       XID: 0/2/CPU0: 4 (0x1280004)
       Bridge ID: 1, Split Horizon ID: 0
       RX TLU1 : 0x4c03
       RX TLU2
                : 0x1013c03
       RX TLU3
                : 0x200ba03
               : 0x3000c03
       RX TLU4
  INGRESS AC [version, state]: [1, BOUND]
       Xconnect-ID: [4] TCAM-Key: (UIDB:0x2 O-vlan:4 I-vlan:0 Ether-Type:0x8100)
       HW: 0x24003001 0x01280004 0x10128006 0xc7ff7400
       SW: 0x24003001 0x01280004 0x10128006 0xc7ff7400
       Service type: 4 (bridging pmp)
       Entry type: 1 (fwd)
       Bridge ID: 1
       ACL ID : 4097
       Xconnect ID : 0x1280004
       SplitHorizonGroup ID: 0
       Rewrite supported: 0 (No)
       PW mode: 0 (vc-type 5)
       AC-type: 1 (vlan-mode)
       Interface handle: 0x128006
       Ingress AC stats: 0x7ff74
```

```
SMAC Learning: enable
DMAC Flooding: enable

Nbor 5.0.0.5 pw-id 2
Number of MAC: 0
Statistics:
  packets: received 0, sent 0
  bytes: received 0, sent 0

INGRESS BRIDGE PORT [version, state]: [1, BOUND]
  Bridge Port Type: ATOM
  XID: 127/15/CPU0: 2 (0xfff80002)
  Bridge ID: 1, Split Horizon ID: 1
  VC label: 16008
  Control-word supported: No
```

The following sample output shows the hardware information of the route processor, for a specific bridge-domain on the ingress detail location:

RP/0/RP0/CPU0:router#show l2vpn forwarding bridge-domain hardware ingress detail location 0/RP0/CPU0

```
Bridge-domain name: aa:g1, 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
Bridge MTU: 1500 bytes
Number of bridge ports: 4
Number of MAC addresses: 0
Multi-spanning tree instance: 0
   BRIDGE [version, state]: [1, CREATED]
       Bridge ID: 0
        FGID1: 44032
                      NodeCount: 1 Info_len: 24 XID_count: 4
        FGID2: 44033
                      NodeCount: 1 Info len: 20 XID count: 3
       FGID1 Membership list:
        node-id: 0/2/CPU0 (0x21) RSI: 0x25 XID count: 4
                                              0x1280003
                                                            0xfff80001
         XID: 0x1280001 0x1280002
       FGID2 Membership list:
        node-id: 0/2/CPU0 (0x21) RSI: 0x25
                                              XID count: 3
         XID: 0x1280001
                             0x1280002
                                              0x1280003
  GiqabitEthernet0/2/0/1.1, state: oper up
   Number of MAC: 0
   Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  AC [version, state]: [1, BOUND]
       XID: 0x1280001 RSI: 0x25
                                   Bridging: TRUE
  GigabitEthernet0/2/0/1.2, state: oper up
   Number of MAC: 0
```

```
Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  AC [version, state]: [1, BOUND]
       XID: 0x1280002 RSI: 0x25
                                   Bridging: TRUE
  GigabitEthernet0/2/0/1.3, state: oper up
   Number of MAC: 0
   Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  AC [version, state]: [1, BOUND]
       XID: 0x1280003 RSI: 0x25
                                   Bridging: TRUE
 Nbor 5.0.0.5 pw-id 1
   Number of MAC: 0
Bridge-domain name: aa:g2, id: 1, 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
Bridge MTU: 1500 bytes
Number of bridge ports: 2
Number of MAC addresses: 0
Multi-spanning tree instance: 0
  BRIDGE [version, state]: [1, CREATED]
       Bridge ID: 1
        FGID1: 44034
                       NodeCount: 1 Info len: 16 XID count: 2
        FGID2: 44035 NodeCount: 1 Info_len: 12 XID_count: 1
       FGID1 Membership list:
        node-id: 0/2/CPU0 (0x21) RSI: 0x25
                                              XID count: 2
         XID: 0x1280004
                          0xfff80002
       FGID2 Membership list:
        node-id: 0/2/CPU0 (0x21) RSI: 0x25
                                              XID count: 1
         XID: 0x1280004
  GigabitEthernet0/2/0/1.4, state: oper up
   Number of MAC: 0
   Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  AC [version, state]: [1, BOUND]
       XID: 0x1280004 RSI: 0x25 Bridging: TRUE
  Nbor 5.0.0.5 pw-id 2
   Number of MAC: 0
```

The following sample output shows the hardware information of the line card, for a specific bridge-domain on the egress detail location:

RP/0/RP0/CPU0:router#show l2vpn forwarding bridge-domain hardware egress detail location 0/2/CPU0

```
Bridge-domain name: aa:gl, 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
Bridge MTU: 1500 bytes
Number of bridge ports: 4
 Number of MAC addresses: 0
Multi-spanning tree instance: 0
  EGRESS BRIDGE [version, state]: [1, CREATED]
        BID: 0 Total_oif_count: 4
AC: oif_count: 3 head_ptr: 0x9ff6e4f8 tail_ptr: 0x9ff6e480
        PW: oif count: 1 head ptr: 0x9ff6e570
        PLU RESULT Key[Bridge-ID: 0]
        HW: 0x04008000 0x000a01c0 0x00000000 0x00000000
        SW: 0x04008000 0x000a01c0 0x00000000 0x00000000
        Entry_type: 1
        OLIST pointer: 0xa01
        OLIST channel: 3
        OLIST count: 4
        OIF[0] seg type: AC xid: 0x1280003 Gi0/2/0/1.3 (ifh: 0x1280042)
        TLU RESULT tlu addr: 0x3000a01 ch: 3 seg type: 1
        HW: 0x80000002 0x00ba0080 0x01280003 0x00000000
        SW: 0x80000002 0x00ba0080 0x01280003 0x00000000
        SHG: 0
        UIDB: 2
        XID: 0x1280003
        OLIST pointer: 0xba00
        OLIST channel: 2
        OIF[1] seg type: AC xid: 0x1280002 Gi0/2/0/1.2 (ifh: 0x1280022)
        TLU RESULT tlu addr: 0x200ba00 ch: 2 seg type: 1
        HW: 0x80000002 0x000a00c0 0x01280002 0x00000000
        SW: 0x80000002 0x0000a00c0 0x01280002 0x00000000
        SHG: 0
        UIDB: 2
        XID: 0x1280002
        OLIST pointer: 0xa00
        OLIST channel: 3
        OIF[2] seg_type: AC xid: 0x1280001 Gi0/2/0/1.1 (ifh: 0x1280002)
        TLU RESULT tlu addr: 0x3000a00 ch: 3 seg type: 1
        HW: 0x80000002 0x00ba0180 0x01280001 0x00000000
        SW: 0x80000002 0x00ba0180 0x01280001 0x00000000
        SHG: 0
        UIDB: 2
        XID: 0x1280001
        OLIST pointer: 0xba01
```

```
OLIST channel: 2
     OIF[3] seg_type: PW xid: 0xfff80001 ecd_ptr: 0x5206
      TLU RESULT tlu addr: 0x200ba01 ch: 2 seg type: 0
     HW: 0x01005206 0x00000000 0xfff80001 0x03e86000
      SW: 0x01005206 0x00000000 0xfff80001 0x03e86000
      SHG: 1
     XID: 0xfff80001
     OLIST pointer: 0x0
     OLIST channel: 0
     Control Word: Disabled
      VC label: 16006
     ECD/TLU1 pointer: 0x5206
GigabitEthernet0/2/0/1.1, state: oper up
 Number of MAC: 0
  Statistics:
   packets: received 0, sent 0
   bytes: received 0, sent 0
EGRESS BRIDGE PORT [version, state]: [1, BOUND]
     Bridge Port Type: AC
      XID: 0/2/CPU0: 1 (0x1280001)
     Bridge ID: 0, Split Horizon ID: 0
     RX TLU1 : 0x4c00
     RX TLU2 : 0x1013c00
     RX TLU3 : 0x200ba00
     RX TLU4 : 0x3000c00
 EGRESS AC [version, state]: [1, BOUND]
     Xconnect-ID: [1] TLU2-entry-addr: [0x200a001]
      HW: 0x8018b000 0x0000000b 0x00004001 0xfb7ba000
      SW: 0x8018b000 0x0000000b 0x00004001 0xfb7ba000
     Entry status: 1 (Fwd)
     AC type: 1 (vlan-mode)
     Outer-vlan: 1
      Inner-vlan: 0
      Outer Ether Type: 0 (dot1q)
     AC mtu: 1580
     Adjacency type: 0
      Default EgressQ (SharqQ): 11
      PW mode: 0 (vc-type 5)
      Rewrite supported: 0 (No)
     Control-word supported: 0 (No)
      Egress AC stats: 0x7dbdd
GigabitEthernet0/2/0/1.2, state: oper up
 Number of MAC: 0
  Statistics:
   packets: received 0, sent 0
   bytes: received 0, sent 0
EGRESS BRIDGE PORT [version, state]: [1, BOUND]
     Bridge Port Type: AC
     XID: 0/2/CPU0 : 2 (0x1280002)
     Bridge ID: 0, Split Horizon ID: 0
     RX TLU1 : 0x4c01
              : 0x1013c01
     RX TLU2
               : 0x200ba01
     RX TLU3
     RX TLU4 : 0x3000c01
```

```
EGRESS AC [version, state]: [1, BOUND]
      Xconnect-ID: [2] TLU2-entry-addr: [0x200a002]
      HW: 0x8018b000 0x0000000b 0x00004002 0xfb7b4000
      SW: 0x8018b000 0x0000000b 0x00004002 0xfb7b4000
      Entry status: 1 (Fwd)
     AC type: 1 (vlan-mode)
     Outer-vlan: 2
     Inner-vlan: 0
     Outer Ether Type: 0 (dot1q)
     AC mtu: 1580
      Adjacency type: 0
      Default EgressQ (SharqQ): 11
      PW mode: 0 (vc-type 5)
     Rewrite supported: 0 (No)
      Control-word supported: 0 (No)
      Egress AC stats: 0x7dbda
GigabitEthernet0/2/0/1.3, state: oper up
 Number of MAC: 0
  Statistics:
   packets: received 0, sent 0
   bytes: received 0, sent 0
EGRESS BRIDGE PORT [version, state]: [1, BOUND]
     Bridge Port Type: AC
     XID: 0/2/CPU0 : 3 (0x1280003)
     Bridge ID: 0, Split Horizon ID: 0
     RX TLU1 : 0x4c02
     RX TLU2
              : 0x1013c02
              : 0x200ba02
     RX TLU3
     RX TLU4
               : 0x3000c02
EGRESS AC [version, state]: [1, BOUND]
      Xconnect-ID: [3] TLU2-entry-addr: [0x200a003]
      HW: 0x8018b000 0x0000000b 0x00004003 0xfb7ae000
      SW: 0x8018b000 0x0000000b 0x00004003 0xfb7ae000
     Entry status: 1 (Fwd)
      AC type: 1 (vlan-mode)
     Outer-vlan: 3
      Inner-vlan: 0
     Outer Ether Type: 0 (dot1q)
     AC mtu: 1580
      Adjacency type: 0
     Default EgressQ (SharqQ): 11
      PW mode: 0 (vc-type 5)
      Rewrite supported: 0 (No)
      Control-word supported: 0 (No)
      Egress AC stats: 0x7dbd7
Nbor 5.0.0.5 pw-id 1
 Number of MAC: 0
 Statistics:
   packets: received 0, sent 0
   bytes: received 0, sent 0
EGRESS BRIDGE PORT [version, state]: [1, BOUND]
     Bridge Port Type: ATOM
```

```
XID: 127/15/CPU0 : 1 (0xfff80001)
        Bridge ID: 0, Split Horizon ID: 1
        VC label: 16006
        Control-word supported: No
Bridge-domain name: aa:g2, id: 1, 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
 Bridge MTU: 1500 bytes
Number of bridge ports: 2
Number of MAC addresses: 0
Multi-spanning tree instance: 0
  EGRESS BRIDGE [version, state]: [1, CREATED]
        BID: 1 Total oif count: 2
        AC: oif count: 1 head ptr: 0x9ff6e534 tail ptr: 0x9ff6e534
        PW: oif count: 1 head ptr: 0x9ff6e5ac
        PLU RESULT Key[Bridge-ID: 1]
        HW: 0x04004000 0x000a02c0 0x00000000 0x00000000
        SW: 0x04004000 0x000a02c0 0x00000000 0x00000000
        Entry type: 1
        OLIST pointer: 0xa02
        OLIST channel: 3
        OLIST count: 2
        OIF[0] seg type: AC xid: 0x1280004 Gi0/2/0/1.4 (ifh: 0x1280062)
        TLU RESULT tlu addr: 0x3000a02 ch: 3 seg type: 1
        HW: 0x80000002 0x00ba0280 0x01280004 0x00000000
        SW: 0x80000002 0x00ba0280 0x01280004 0x00000000
        SHG: 0
        UIDB: 2
        XID: 0x1280004
        OLIST pointer: 0xba02
        OLIST channel: 2
        OIF[1] seg_type: PW xid: 0xfff80002 ecd ptr: 0x5200
        TLU RESULT tlu addr: 0x200ba02 ch: 2 seg type: 0
        HW: 0x01005200 0x00000000 0xfff80002 0x03e88000
        SW: 0x01005200 0x00000000 0xfff80002 0x03e88000
        SHG: 1
        XID: 0xfff80002
        OLIST pointer: 0x0
        OLIST channel: 0
        Control Word: Disabled
        VC label: 16008
        ECD/TLU1 pointer: 0x5200
  GigabitEthernet0/2/0/1.4, state: oper up
   Number of MAC: 0
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
```

```
EGRESS BRIDGE PORT [version, state]: [1, BOUND]
      Bridge Port Type: AC
     XID: 0/2/CPU0 : 4 (0x1280004)
      Bridge ID: 1, Split Horizon ID: 0
      RX TLU1 : 0x4c03
              : 0x1013c03
      RX TLU2
      RX TLU3
               : 0x200ba03
              : 0x3000c03
      RX TLU4
 EGRESS AC [version, state]: [1, BOUND]
      Xconnect-ID: [4] TLU2-entry-addr: [0x200a004]
      HW: 0x8018b000 0x0000000b 0x00004004 0xfb7a8000
      SW: 0x8018b000 0x0000000b 0x00004004 0xfb7a8000
      Entry status: 1 (Fwd)
      AC type: 1 (vlan-mode)
      Outer-vlan: 4
      Inner-vlan: 0
      Outer Ether Type: 0 (dot1q)
      AC mtu: 1580
      Adjacency_type: 0
      Default EgressQ (SharqQ): 11
      PW mode: 0 (vc-type 5)
      Rewrite supported: 0 (No)
      Control-word supported: 0 (No)
      Egress AC stats: 0x7dbd4
Nbor 5.0.0.5 pw-id 2
 Number of MAC: 0
  Statistics:
   packets: received 0, sent 0
   bytes: received 0, sent 0
EGRESS BRIDGE PORT [version, state]: [1, BOUND]
      Bridge Port Type: ATOM
      XID: 127/15/CPU0 : 2 (0xfff80002)
      Bridge ID: 1, Split Horizon ID: 1
      VC label: 16008
      Control-word supported: No
```

This table describes the significant fields shown in the display.

Table 13: show I2vpn 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 146	Clears the MAC addresses and restarts the bridge domains on the router.

# show I2vpn 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	Displays detailed information for the MAC address.			
hardware	Reads inf	Reads information from the hardware.			
egress	Reads inf	Formation from the egress PSE.			
ingress	Reads inf	Formation from the ingress PSE.			
interface	Displays	Displays the match for the attachment circuit subinterface.			
type	Interface	Interface type. For more information, use the question mark (?) online help function.			
interface-path-id	Physical interface or virtual interface.				
	Note	Use the <b>show interfaces</b> command to see a list of all interfaces currently configured on the router.			
	For more help func	information about the syntax for the router, use the question mark (?) online tion.			
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 <i>node-id</i> argument is entered in the <i>rack/slot/module</i> 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
12vpn	read

## **Examples**

The following sample output shows the specified location of the bridge-domain name g1:bd1 for the MAC address:

```
        RP/0/RP0/CPU0:router# show 12vpn
        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/RP0/CPU0:router# show 12vpn 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/RP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 mac-address 1.2.3 location
0/1/CPU0

The following sample output shows the hardware information from the egress pse:

RP/0/RP0/CPU0:router# show 12vpn forwarding bridge-domain g1:bd1 mac-address hardware egress

#### location 0/1/CPU0

Mac Address	Туре	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/RP0/CPU0:router# show 12vpn 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	9		
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.

## $\label{eq:reduced_reduced_reduced} $$RP/0/RP0/CPU0:$ router $\#$ show 12vpn forwarding bridge-domain $g1:bd1 mac-address interface gigabitEthernet 0/1/0/0 location 0/1/CPU0 $$$

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	-		0/1/CPU0	0d 0h 2m 14s
0000.0001.0112	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 14s
0000.0001.0113	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 14s
0000.0001.0114	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 14s

The following sample output shows the MAC address hardware information on the line card, for a specific bridge-domain on the ingress detail location:

## RP/0/RP0/CPU0:router#show 12vpn forwarding bridge-domain mac hardware ingress detail location 0/2/CPU0

```
Bridge-domain name: aa:g1, 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
Bridge MTU: 1500 bytes
Number of bridge ports: 4
Number of MAC addresses: 10
Multi-spanning tree instance: 0
  INGRESS BRIDGE [version, state]: [1, CREATED]
        TCAM entry seq#: 1024 Key: [BID: 0 MAC: default]
        HW: 0x4c000000 0x000080ac 0x00010000 0x80ac0100
        SW: 0x4c000000 0x000080ac 0x00010000 0x80ac0100
        SMAC: action: PUNT state: NO REFRESH
        DMAC: action: FLOOD, flood enable: enable
        FGID: All: 44032, VFI: 44033, MCAST_Sponge_q: 16
        Fabric multicast1: 1 Fabric multicast2: 1
        Admin State: UP
        MTU: 1500
```

```
Number of MAC addresses: 11 (10 MAC + 1 default)
       ACL NAME (ACL-ID): VPLS Special (4096)
       TCAM region handle : 5
 GigabitEthernet0/2/0/1.1, state: oper up
   Number of MAC: 10
   Statistics:
    packets: received 0, sent 121515
    bytes: received 0, sent 7290900
 INGRESS BRIDGE PORT [version, state]: [1, BOUND]
      Bridge Port Type: AC
      XID: 0/2/CPU0 : 1 (0x1280001)
      Bridge ID: 0, Split Horizon ID: 0
      RX TLU1 : 0x4c00
                : 0x1013c00
      RX TLU2
                : 0x200ba00
       RX TLU3
      RX TLU4
               : 0x3000c00
  INGRESS AC [version, state]: [1, BOUND]
       Xconnect-ID: [1] TCAM-Key: (UIDB:0x2 O-vlan:1 I-vlan:0 Ether-Type:0x8100)
      HW: 0x24001000 0x01280001 0x10128000 0xc7ff7d00
       SW: 0x24001000 0x01280001 0x10128000 0xc7ff7d00
       Service type: 4 (bridging pmp)
       Entry type: 1 (fwd)
       Bridge_ID : 0
      ACL_ID : 4096
      Xconnect ID: 0x1280001
       SplitHorizonGroup ID : 0
      Rewrite supported: 0 (No)
       PW mode: 0 (vc-type 5)
      AC-type: 1 (vlan-mode)
       Interface handle: 0x128000
       Ingress AC stats: 0x7ff7d
       SMAC Learning: enable
       DMAC Flooding: enable
Mac Address: 0000.0022.2222, LC learned: 0/2/CPU0
 Age: 0d 0h 0m 21s, Flag: local
 INGRESS MAC [version, state]: [1, CREATED]
       TCAM entry seq#: 0 Key: [BID: 0 MAC: 0000.0022.2222]
       HW: 0x22004c00 0x00000001 0x00000000 0x01280001
       SW: 0x22004c00 0x00000001 0x00000000 0x01280001
       SMAC: action: FWD state: REFRESH
       XID: 0/2/CPU0 : 1 (0x1280001)
       DMAC: action: FWD, BridgePort type: AC
       SHG ID
               : 0
       Entry Flag : FWD
       Entry Type : DYNAMIC
       Local Switching: enabled
       Next (tlu0) addr: 0x4c00
      Control-word supported: No
       Destination AC: Gi0/2/0/1.1 (ifh: 0x1280002)
       TLU1
                       : 0x4c00
```

```
[HW: 0x00000000 0x00013c00 0x00000000 0x00000100]
           label: 0 num of labels: entry type: FWD next ptr: 0 \times 00001
                                   next ptr: 0x00013c00
           num of entries: 1
           BGP next-hop: 0.0.0.0
                      : 0x1013c00
       [HW: 0x00000008 0x00000000 0x00001000 0x00ba0000]
           label1: 1 label2:
           num of labels:
                                   next ptr: 0x0000ba00
                      : 0x200ba00
       [HW: 0x00010000 0x00000000 0x00000000 0x000c0000]
          num. entries : 1
          num. labels : 0
          label 1 : 0
                      : 0
          label 2
                       : 0xc00
          next ptr
                      : 0x3000c00
       [HW: 0x00000000 0x20082000 0x01280040 0x00020000]
          dest. addr : 0x20
          sponge queue : 130
          egress port : 0x128004
          rp destined : no
          rp drop
                      : no
          hash type
                       : 0
          uidb index : 0x2
Mac Address: 0000.0022.2223, LC learned: 0/2/CPU0
 Age: 0d 0h 0m 21s, Flag: local
 INGRESS MAC [version, state]: [1, CREATED]
       TCAM entry seg#: 1 Key: [BID: 0 MAC: 0000.0022.2223]
       HW: 0x22004c00 0x00000001 0x00000000 0x01280001
       SW: 0x22004c00 0x00000001 0x00000000 0x01280001
       SMAC: action: FWD state: REFRESH
      XID: 0/2/CPU0 : 1 (0x1280001)
       DMAC: action: FWD, BridgePort type: AC
       SHG ID : 0
      Entry Flag : FWD
      Entry Type : DYNAMIC
      Local Switching: enabled
      Next (tlu0) addr: 0x4c00
      Control-word supported: No
       Destination AC: Gi0/2/0/1.1 (ifh: 0x1280002)
                     : 0x4c00
       TI_iU1
       [HW: 0x00000000 0x00013c00 0x00000000 0x00000100]
           label: 0 num of labels: entry type: FWD next ptr: 0x000
                                                          Λ
                                   next ptr: 0x00013c00
           num of entries: 1
           BGP next-hop: 0.0.0.0
       TLU2
                    : 0x1013c00
       [HW: 0x00000008 0x00000000 0x00001000 0x00ba0000]
          label1: 1 label2: num of labels: 1 next ptr: 0x0000b
                                   next ptr: 0x0000ba00
       TLU3
                     : 0x200ba00
```

```
[HW: 0x00010000 0x00000000 0x00000000 0x000c0000]
          num. entries : 1
          num. labels : 0
          label 1
                     : 0
          label 2
          next ptr
                       : 0xc00
                      : 0x3000c00
      TT<sub>i</sub>U4
      [HW: 0x00000000 0x20082000 0x01280040 0x00020000]
          dest. addr : 0x20
          sponge queue : 130
          egress port : 0x128004 rp destined : no
          rp drop
                       : no
          hash type
                     : 0
          uidb index : 0x2
Mac Address: 0000.0022.2224, LC learned: 0/2/CPU0
 Age: Od Oh Om 21s, Flag: local
 INGRESS MAC [version, state]: [1, CREATED]
      TCAM entry seq#: 2 Key: [BID: 0 MAC: 0000.0022.2224]
      HW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SMAC: action: FWD state: REFRESH
      XID: 0/2/CPU0 : 1 (0x1280001)
      DMAC: action: FWD, BridgePort type: AC
      SHG ID : 0
      Entry Flag : FWD
      Entry Type : DYNAMIC
      Local Switching: enabled
      Next (tlu0) addr: 0x4c00
      Control-word supported: No
      Destination AC: Gi0/2/0/1.1 (ifh: 0x1280002)
      TLU1
                      : 0x4c00
      [HW: 0x00000000 0x00013c00 0x00000000 0x00000100]
                      0 num of labels:
           label:
           entry type:
                          FWD
                                   next ptr: 0x00013c00
           num of entries: 1
           BGP next-hop: 0.0.0.0
                     : 0x1013c00
      [HW: 0x00000008 0x00000000 0x00001000 0x00ba0000]
           label1: 1 label2:
           num of labels:
                            1
                                   next ptr: 0x0000ba00
                     : 0x200ba00
      TLU3
      [HW: 0x00010000 0x00000000 0x00000000 0x000c0000]
          num. entries : 1
          num. labels : 0
          label 1
          label 2
                       : 0
          next ptr
                      : 0xc00
                      : 0x3000c00
      тт.п4
      [HW: 0x00000000 0x20082000 0x01280040 0x00020000]
          dest. addr : 0x20
          sponge queue : 130
          egress port : 0x128004
```

```
rp destined : no
                    : no
: 0
          rp drop
          hash type
          uidb index : 0x2
Mac Address: 0000.0022.2225, LC learned: 0/2/CPU0
 Age: 0d 0h 0m 21s, Flag: local
 INGRESS MAC [version, state]: [1, CREATED]
      TCAM entry seq#: 3 Key: [BID: 0 MAC: 0000.0022.2225]
      HW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SMAC: action: FWD state: REFRESH
      XID: 0/2/CPU0 : 1 (0x1280001)
      DMAC: action: FWD, BridgePort type: AC
      SHG ID : 0
      Entry Flag : FWD
      Entry Type : DYNAMIC
      Local Switching: enabled
      Next (tlu0) addr: 0x4c00
      Control-word supported: No
      Destination AC: Gi0/2/0/1.1 (ifh: 0x1280002)
      TLU1
                      : 0x4c00
       [HW: 0x00000000 0x00013c00 0x00000000 0x00000100]
          label: 0 num of labels: entry type: FWD next ptr: 0x000
                                  next ptr: 0x00013c00
           num of entries: 1
           BGP next-hop: 0.0.0.0
                   : 0x1013c00
      TT.II2
       [HW: 0x00000008 0x00000000 0x00001000 0x00ba0000]
          label1: 1
                                  label2: 0
           num of labels: 1
                                  next ptr: 0x0000ba00
                      : 0x200ba00
       [HW: 0x00010000 0x00000000 0x00000000 0x000c0000]
         num. entries : 1
          num. labels : 0
          label 1 : 0
                      : 0
: 0xc00
          label 2
          next ptr
                      : 0x3000c00
       [HW: 0x00000000 0x20082000 0x01280040 0x00020000]
         dest. addr : 0x20
          sponge queue : 130
          egress port : 0x128004
          rp destined : no
                     : no
          rp drop
          hash type
                      : 0
                     : 0x2
          uidb index
Mac Address: 0000.0022.2226, LC learned: 0/2/CPU0
 Age: 0d 0h 0m 21s, Flag: local
 INGRESS MAC [version, state]: [1, CREATED]
      TCAM entry seq#: 4 Key: [BID: 0 MAC: 0000.0022.2226]
```

```
HW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SMAC: action: FWD state: REFRESH
      XID: 0/2/CPU0 : 1 (0x1280001)
      DMAC: action: FWD, BridgePort type: AC
                : 0
      SHG ID
      Entry Flag : FWD
      Entry Type : DYNAMIC
      Local Switching: enabled
      Next (tlu0) addr: 0x4c00
      Control-word supported: No
      Destination AC: Gi0/2/0/1.1 (ifh: 0x1280002)
                     : 0x4c00
      TLU1
       [HW: 0x00000000 0x00013c00 0x00000000 0x00000100]
           label:
                            0
                                  num of labels:
           entry type:
                           FWD
                                   next ptr: 0x00013c00
           num of entries: 1
           BGP next-hop: 0.0.0.0
                      : 0x1013c00
       [HW: 0x00000008 0x00000000 0x00001000 0x00ba0000]
           label1: 1 label2:
           num of labels:
                            1
                                   next ptr: 0x0000ba00
      TLU3
                      : 0x200ba00
       [HW: 0x00010000 0x00000000 0x00000000 0x000c0000]
         num. entries : 1
          num. labels : 0
          label 1 : 0
          label 2
                      : 0
          next ptr
                      : 0xc00
                      : 0x3000c00
       [HW: 0x00000000 0x20082000 0x01280040 0x00020000]
          dest. addr : 0x20
          sponge queue : 130
          egress port
                       : 0x128004
          rp destined : no
          rp drop : no
          hash type
                      : 0
          uidb index : 0x2
Mac Address: 0000.0022.2227, LC learned: 0/2/CPU0
 Age: 0d 0h 0m 21s, Flag: local
 INGRESS MAC [version, state]: [1, CREATED]
      TCAM entry seq#: 5 Key: [BID: 0 MAC: 0000.0022.2227]
      HW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SMAC: action: FWD state: REFRESH
      XID: 0/2/CPU0 : 1 (0x1280001)
      DMAC: action: FWD, BridgePort type: AC
      SHG ID : 0
      Entry Flag : FWD
      Entry Type : DYNAMIC
      Local Switching: enabled
      Next (tlu0) addr: 0x4c00
      Control-word supported: No
```

```
Destination AC: Gi0/2/0/1.1 (ifh: 0x1280002)
      רד.דד1
                    : 0x4c00
       [HW: 0x00000000 0x00013c00 0x00000000 0x00000100]
           label: 0 num of labels:
                           FWD
                                   next ptr: 0x00013c00
           entry type:
           num of entries: 1
           BGP next-hop: 0.0.0.0
      TLU2
                   : 0x1013c00
       [HW: 0x00000008 0x00000000 0x00001000 0x00ba0000]
           label1: 1 label2: 0 num of labels: 1 next ptr: 0x0000ba00
                                   next ptr: 0x0000ba00
                     : 0x200ba00
      TLU3
      [HW: 0x00010000 0x00000000 0x00000000 0x000c0000]
          num. entries : 1
          num. labels : 0
          label 1 : 0
          label 2
                       : 0
          next ptr : 0xc00
                    : 0x3000c00
      TT.II4
       [HW: 0x00000000 0x20082000 0x01280040 0x00020000]
          dest. addr : 0x20
          sponge queue : 130
          egress port : 0x128004 rp destined : no
          rp drop
                        : no
                      : 0
          hash type
          uidb index : 0x2
Mac Address: 0000.0022.2228, LC learned: 0/2/CPU0
 Age: 0d 0h 0m 21s, Flag: local
 INGRESS MAC [version, state]: [1, CREATED]
      TCAM entry seq#: 6 Key: [BID: 0 MAC: 0000.0022.2228]
      HW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SW: 0x22004c00 0x00000001 0x00000000 0x01280001
      SMAC: action: FWD state: REFRESH
      XID: 0/2/CPU0 : 1 (0x1280001)
      DMAC: action: FWD, BridgePort type: AC
      SHG ID : 0
      Entry Flag : FWD
      Entry Type : DYNAMIC
      Local Switching: enabled
      Next (tlu0) addr: 0x4c00
      Control-word supported: No
      Destination AC: Gi0/2/0/1.1 (ifh: 0x1280002)
      TLU1
                      : 0x4c00
       [HW: 0x00000000 0x00013c00 0x00000000 0x00000100]
           label: 0 num of labels: entry type: FWD next ptr: 0x0001
                                    next ptr: 0x00013c00
           num of entries: 1
           BGP next-hop: 0.0.0.0
      TLU2
                      : 0 \times 1013 c \cdot 00
       [HW: 0x00000008 0x00000000 0x00001000 0x00ba0000]
```

```
label1:
                              1
                                     label2:
            num of labels:
                             1
                                     next ptr: 0x0000ba00
       TLU3
                      : 0x200ba00
       [HW: 0x00010000 0x00000000 0x00000000 0x000c0000]
          num. entries : 1
          num. labels : 0 label 1 : 0 label 2 : 0
          next ptr : 0xc00
                       : 0x3000c00
       [HW: 0x00000000 0x20082000 0x01280040 0x00020000]
          dest. addr : 0x20
           sponge queue : 130
           egress port : 0x128004
           rp destined : no
                     : no
: 0
           rp drop
           hash type
           uidb index : 0x2
Mac Address: 0000.0022.2229, LC learned: 0/2/CPU0
```

Age: Od Oh Om 21s, Flag: local

#### **Related Commands**

Command	Description		
show I2vpn forwarding bridge-domain (VPLS), on page 180	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 3.8.0	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.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# shutdown
```

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	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 3.8.0	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
12vpn	read, write

#### **Examples**

The following example shows how to disable VFI:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# vfi v1
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-vfi)# shutdown

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 44	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 159	Configures the MPLS static labels and the static labels for the access pseudowire configuration.

Command	Description
neighbor (VPLS), on page 163	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 3.8.0	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 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac)# static-address 1.1.1 drop

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
mac (VPLS), on page 155	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 3.8.0	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
12vpn	read, write

#### **Examples**

The following example shows how to associate a remote MAC address with a pseudowire:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# vfi model
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-12vpn-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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd) # interface GigabitEthernet 0/1/0/0
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# neighbor 10.1.1.2 pw-id 2000
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-pw)# static-mac-address 2.2.2
```

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 44	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 159	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 163	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
vfi (VPLS), on page 218	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 3.8.0	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.

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac)# aging
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac-aging)# time 600

Command	Description
aging (VPLS), on page 142	Enters the MAC aging configuration submode to set the aging parameters such as time and type.

Description
Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
Enters L2VPN configuration mode.
Enters L2VPN bridge group bridge domain MAC configuration mode.
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 3.8.0	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.

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
12vpn	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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac

RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# type absolute

Command	Description
aging (VPLS), on page 142	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
mac (VPLS), on page 155	Enters L2VPN bridge group bridge domain MAC configuration mode.
time (VPLS), on page 214	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 3.8.0	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 **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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# vfi v1
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-vfi)#

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 159	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 163	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 3.8.0	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
12vpn	read, write

#### **Examples**

The following example shows how to enable disable MAC withdrawal:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-12vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-12vpn-bg-bd-mac)# withdraw disable
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 12vpn
RP/0/RP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
```

RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)# withdraw access-pw disable

Command	Description
bridge-domain (VPLS), on page 144	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 145	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
I2vpn, on page 44	Enters L2VPN configuration mode.
mac (VPLS), on page 155	Enters L2VPN bridge group bridge domain MAC configuration mode.

withdraw (VPLS)



## **Generic Routing Encapsulation Commands**

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

For detailed information about GRE concepts, configuration tasks, and examples, refer to the .

- interface tunnel-ip, on page 224
- keepalive, on page 225
- tunnel destination, on page 226
- tunnel dfbit, on page 227
- tunnel mode, on page 228
- tunnel source, on page 229
- tunnel tos, on page 231
- tunnel ttl, on page 232

## interface tunnel-ip

To configure a tunnel interface, use the **interface tunnel-ip** command in the interface global configuration mode. To disable this feature, use the **no** form of this command.

interface tunnel-ip number
no interface tunnel-ip number

#### **Syntax Description**

number Specifies the instance number of the interface to be configured.

#### **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.

Use the **interface tunnel-ip** command to enter the interface global configuration mode.

#### Task ID

Task ID	Operations
interface	read, write

#### **Examples**

This example shows how to configure a tunnel interface:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RP0/CPU0:router(config-if)#

## keepalive

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

keepalive [time\_in\_seconds [retry\_num]]
no keepalive

#### **Syntax Description**

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

#### **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.

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

#### Task ID

Task ID	Operations
interface	read, write

#### **Examples**

The following example shows how to configure interface tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RP0/CPU0:router(config-if)# keepalive 30
```

## tunnel destination

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



Note

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

tunnel destination ip-address no tunnel destination ip-address

#### **Syntax Description**

*ip-address* Specifies the IPv4 address of the host destination.

#### **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.

#### Task ID

Task ID	Operations
interface	read, write

#### **Examples**

The following example shows how to configure interface tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RP0/CPU0:router(config-if)# tunnel destination 10.10.10.1
```

Command	Description
tunnel mode, on page 228	Configures the encapsulation mode of the tunnel interface.
tunnel source, on page 229	Sets a tunnel interface's source address.
tunnel tos, on page 231	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 232	Configures the Time-To-Live (TTL) for packets entering the tunnel.

## tunnel dfbit

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

#### tunnel dfbit disable no tunnel dfbit

#### **Syntax Description**

#### **Syntax Description**

**disable** Disables the DF bit in the outer packet. This allows the outer packet to be fragmented, if required.

#### **Command Default**

The DF bit value in the outer packet is disabled. This allows outer packet fragmentation, if required.

#### **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.

#### Task ID

# interface read, write

#### **Examples**

The following example shows how to enable fragmentation over an interface tunnel.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RP0/CPU0:router(config-if)# tunnel dfbit disable
```

Command	Description
tunnel destination, on page 226	Specifies a tunnel interface's destination address.
tunnel mode, on page 228	Configures the encapsulation mode of the tunnel interface.
tunnel source, on page 229	Sets a tunnel interface's source address.
tunnel tos, on page 231	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 232	Configures the Time-To-Live (TTL) for packets entering the tunnel.

## tunnel mode

To configure the encapsulation mode of the tunnel interface, use the **tunnel mode** command. To revert the encapsulation to the default IPv4 GRE tunnel mode, use the **no** form of this command.

tunnel mode gre ipv4} no tunnel mode

<b>Syntax</b>	Description
Syntax	Description

gre	ipv4	Specifies the tunnel as a GRE
		tunnel over an IPv4 transport
		network.

#### **Command Default**

The default tunnel mode is set as a GRE tunnel over an IPv4 transport network.

#### **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.

#### Task ID

# interface read, write

#### **Examples**

The following example shows how to configure interface tunnel:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RP0/CPU0:router(config-if)#tunnel mode gre ipv4

Command	Description	
tunnel destination, on page 226	Specifies a tunnel interface's destination address.	
tunnel source, on page 229	Sets a tunnel interface's source address.	
tunnel tos, on page 231	Specifies the value of the TOS field in the tunnel encapsulating packets.	
tunnel ttl, on page 232	Configures the Time-To-Live (TTL) for packets entering the tunnel.	

## tunnel source

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



#### Note

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

tunnel source {interface\_name | ip-address}
no tunnel source {interface\_name | ip-address}

#### **Syntax Description**

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

#### **Command Default**

None

#### **Command Modes**

interface configuration

#### **Command History**

Release	Modification	
Release 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.

It is recommended that the tunnel source is identified using the interface ID and not the IP address. Using the interface ID enables the router to mark the tunnel as down when the interface is down and the routing protocol tries to find and use an alternate route to the tunnel route.

#### Task ID

## interface read, write

#### **Examples**

The following example shows how to configure interface tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RP0/CPU0:router(config-if)# tunnel source 10.10.10.1
```

Command	Description
tunnel destination, on page 226	Specifies a tunnel interface's destination address.
tunnel mode, on page 228	Configures the encapsulation mode of the tunnel interface.
tunnel tos, on page 231	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 232	Configures the Time-To-Live (TTL) for packets entering the tunnel.

## tunnel tos

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

tunnel tos tos\_value no tunnel tos tos value

#### **Syntax Description**

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

#### **Command Default**

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

#### **Command Modes**

interface configuration

#### **Command History**

Release	Modification
Release 3.9.0	This command was introduced.

#### **Usage Guidelines**

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

#### Task ID

Task ID	Operations
interface	read, write

#### **Examples**

The following example shows how to configure interface tunnel:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RP0/CPU0:router(config-if)# tunnel tos 100

Command	Description
tunnel destination, on page 226	Specifies a tunnel interface's destination address.
tunnel mode, on page 228	Configures the encapsulation mode of the tunnel interface.
tunnel source, on page 229	Sets a tunnel interface's source address.
tunnel ttl, on page 232	Configures the Time-To-Live (TTL) for packets entering the tunnel.

## tunnel ttl

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

tunnel ttl ttl\_value no tunnel ttl ttl value

#### **Syntax Description**

*ttl\_value* Specifies the value of TTL for packets entering the tunnel. The TTL value ranges between 1 to 255.

#### **Command Default**

The default TTL value is set to 255.

#### **Command Modes**

interface configuration

#### **Command History**

Release	Modification
Release 3.9.0	This command was introduced.

#### **Usage Guidelines**

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

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

#### Task ID

Task ID	Operations
interface	read, write

#### **Examples**

The following example shows how to configure interface tunnel:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 400
RP/0/RP0/CPU0:router(config-if)#tunnel source 10.10.10.1

Command	Description
tunnel destination, on page 226	Specifies a tunnel interface's destination address.
tunnel mode, on page 228	Configures the encapsulation mode of the tunnel interface.
tunnel tos, on page 231	Specifies the value of the TOS field in the tunnel encapsulating packets.

Command	Description
tunnel source, on page 229	Sets a tunnel interface's source address.

tunnel ttl