

VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers

First Published: 2022-07-01

Last Modified: 2026-09-11

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

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface xi

Preface xi

Communications, Services, and Additional Information xi

CHAPTER 1

Ethernet Interfaces Commands 1

dot1q tunneling ethertype 2

encapsulation default 4

encapsulation dot1ad dot1q 6

encapsulation dot1q 8

encapsulation dot1q second-dot1q 10

encapsulation untagged 12

ethernet egress-filter 14

ethernet filtering 15

ethernet source bypass egress-filter 18

l2protocol (Ethernet) 19

l2transport (Ethernet) 21

local-traffic default encapsulation 23

rewrite ingress tag 25

CHAPTER 2

Generic Routing Encapsulation Commands 27

bandwidth 28

description (GRE) 29

hw-module l3 feature gre-lite enable 30

ipv4 address 31

ipv4 mtu (LxVPN) 33

ipv6 address (LxVPN) 34

ipv6 mtu (LxVPN) 35
keepalive 36
mtu (GRE) 37
shutdown (GRE) 38
tunnel destination 39
tunnel key 40
tunnel key-ignore 42
tunnel dfbit 44
tunnel mode 45
tunnel source 46
tunnel tos 48
tunnel ttl 49
tunnel vrf 50

CHAPTER 3 **Point to Point Layer 2 Services Commands** 51
advertise-mac 54
address-family l2vpn mspw 55
bgp 56
backup (L2VPN) 57
backup disable (L2VPN) 59
clear l2route evpn ipv4 61
clear l2route evpn ipv6 62
clear l2route evpn mac 63
clear l2vpn collaborators 64
clear l2vpn counters bridge mac-withdrawal 65
clear l2vpn forwarding counters 66
clear l2vpn forwarding counters bridge-domain mirp-lite 67
clear l2vpn forwarding message counters 68
clear l2vpn forwarding table 69
control-word 70
dynamic-arp-inspection 71
flood mode 73
generic-interface-list 75
global-id (L2VPN) 76

interface (p2p) 77
interworking ipv4 78
ipv4 source 79
l2tp static 80
ip-source-guard 83
l2transport 85
l2transport l2protocol 87
l2transport propagate 89
l2transport service-policy 91
l2vpn 92
l2vpn switchover 93
load-balancing flow 94
load-balancing flow-label 95
load-balancing pw-label 97
logging (l2vpn) 98
logging nsr 99
monitor-session (l2vpn) 100
mpls static label (L2VPN) 101
neighbor (L2VPN) 103
neighbor evpn 105
neighbor routed 106
nsr (L2VPN) 107
option-b-asbr-only 108
pw-routing 109
preferred-path 110
protocol l2tpv3 112
pw-class (L2VPN) 113
pw-class encapsulation l2tpv3 114
pw-class encapsulation mpls 116
pw-ether 118
pw-grouping 120
pw-iw 121
p2p 122
rd (L2VPN) 123

sequencing (L2VPN) 125
show bgp l2vpn evpn 127
show bgp l2vpn mspw 129
show bgp vrf-db 130
show evpn evi ead 131
show evpn internal-label 133
show dci-fabric-interconnect 134
show generic-interface-list 137
show l2tp session 139
show l2tp tunnel 141
show l2vpn 143
show l2vpn atom-db 144
show l2vpn collaborators 147
show l2vpn database 149
show l2vpn discovery 152
show l2vpn forwarding 154
show l2vpn forwarding message counters 161
show l2vpn generic-interface-list 163
show l2vpn index 165
show l2vpn nsr 167
show l2vpn process fsm 169
show l2vpn provision queue 171
show l2vpn pw-class 173
show l2vpn pwhe 175
show l2vpn resource 177
show l2vpn trace 178
show l2vpn xconnect 180
show tech-support l2vpn platform no-statistics 189
source (p2p) 191
storm-control 193
switching-tlv (L2VPN) 196
tag-impose 198
tos (l2vpn) 199
transport mode (L2VPN) 201

transport mode vlan passthrough 203
ttl (l2vpn) 204
vpws-seamless-integration 205
xconnect group 206

CHAPTER 4 **Multipoint Layer 2 Services Commands** 207
action (VPLS) 209
aging (VPLS) 211
aps-channel 213
autodiscovery bgp 215
bridge-domain (VPLS) 216
bridge group (VPLS) 217
clear l2vpn bridge-domain (VPLS) 218
coupled-mode 219
debug l2vpn forwarding platform vpls all location 221
description (G.8032) 222
dhcp ipv4 snoop profile (VPLS) 223
ethernet ring g8032 225
ethernet ring g8032 profile 226
exclusion list 228
flooding disable 229
flooding unknown-unicast disable (VPLS) 231
igmp snooping disable 233
inclusion-list 234
instance (G.8032) 236
interface (VPLS) 237
l2vpn resynchronize forwarding mac-address-table location 239
learning disable (VPLS) 240
level 242
limit (VPLS) 243
mac (VPLS) 245
mac secure 247
maximum (VPLS) 250
monitor interface (port0) 252

monitor interface (port1) 253
mpls static label (VPLS) 254
mtu (VPLS) 256
multicast p2mp 258
neighbor (VPLS) 260
notification (VPLS) 262
open ring 264
port0 interface 265
port1 266
port-down flush disable (VPLS) 267
profile 269
pw-class 270
pw-oam 272
pw-status (L2VPN) 273
route-target 275
routed 277
rpl 278
show ethernet ring g8032 280
show l2vpn bridge-domain (VPLS) 283
show l2vpn ethernet ring g8032 294
show l2vpn forwarding bridge-domain (VPLS) 296
show l2vpn forwarding bridge-domain mac-address (VPLS) 299
show l2vpn forwarding ethernet ring g8032 303
show l2vpn forwarding protection main-interface 305
show l2vpn protection main-interface 307
shutdown (Bridge Domain) 310
shutdown (VFI) 311
signaling-protocol 313
split-horizon group 315
static-address (VPLS) 317
static-mac-address (VPLS) 319
tcn-propagation 321
time (VPLS) 322
transport rsvp-te 324

type (VPLS) 326
vfi (VPLS) 328
withdraw (VPLS) 330

CHAPTER 5 EVPN Commands 333
access-signal out-of-service 334
access-signal 335
advertise gateway-ip-disable 336
advertise-mac 337
clear l2route evpn ipv4 338
clear l2route evpn ipv6 339
clear l2route evpn mac 340
evpn 341
evpn evi 342
evpn evi multicast source-connected 343
ethernet-segment 345
ethernet-segment (evpn) 346
implicit-import 347
interface (EVPN) 348
l2vpn evpn 350
mac-flush 352
mpls static label (EVPN ELAN) 354
mpls static label (EVPN VPWS) 355
neighbor evpn 356
non-revertive 357
revert 358
route-target 360
set advertise-evpn-gw-ip 362
service-carving 363
show evpn ethernet-segment 365
show evpn summary 368
show evpn evi 370
show evpn internal-label 374
weight 376

CHAPTER 6 **Layer 2 Access List Commands** 377

copy access-list ethernet-service 378

deny (ES ACL) 380

ethernet-service access-group 383

ethernet-services access-list 385

permit (ES ACL) 387

resequence access-list ethernet-service 390

show access-lists ethernet-services 392

show access-lists ethernet-services trace 396

show access-list ethernet-service usage pfilter 398

show lpts pifib hardware entry optimized 400

CHAPTER 7 **VXLAN Commands** 401

anycast source-interface loopback 402

interface nve 403

member 404

member vni 406

overlay-encapsulation 407

show nve interface 408

show nve peers 409

show nve vni 410

source-interface loopback 411



Preface

The *VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers* preface contains these sections:

- Preface, on page xi
- Communications, Services, and Additional Information, on page xi

Preface

Initial release of the cumulative command reference document that covers all updates from Release 4.1.0 onwards.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results 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.



Ethernet Interfaces Commands

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

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

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

- dot1q tunneling ethertype, on page 2
- encapsulation default, on page 4
- encapsulation dot1ad dot1q, on page 6
- encapsulation dot1q, on page 8
- encapsulation dot1q second-dot1q, on page 10
- encapsulation untagged, on page 12
- ethernet egress-filter, on page 14
- ethernet filtering, on page 15
- ethernet source bypass egress-filter, on page 18
- l2protocol (Ethernet), on page 19
- l2transport (Ethernet), on page 21
- local-traffic default encapsulation, on page 23
- rewrite ingress tag, on page 25

dot1q tunneling ethertype

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

dot1q tunneling ethertype {**0x9100** | **0x9200**}
no dot1q tunneling ethertype

Syntax Description

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

Command Default

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

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
vlan	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
RP/0/RSP0/CPU0:router(config-if)# dot1q tunneling ethertype 0x9100
RP/0/RSP0/CPU0:router(config-if)#
```

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

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

```
RP/0/RSP0/CPU0:router(config-if)# dot1q tunneling ethertype 0x9200
RP/0/RSP0/CPU0:router(config-if)#
```

Related Commands

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

encapsulation default

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

encapsulation default
no encapsulation default

Syntax Description

This command has no keywords or arguments.

Command Default

No default service instance is configured on the port.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

Only one encapsulation command must be configured per service instance.

Examples

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

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

Related Commands

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

Command	Description
encapsulation untagged, on page 12	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

encapsulation dot1ad dot1q

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

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

Syntax Description

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

Command Default

No matching criteria are defined.

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

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

encapsulation dot1q

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

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

Syntax Description

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

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

When encapsulation dot1q is configured with a VLAN range (for example, dot1q 100 second-dot1q A-B or dot1q A-B), the supported number of Layer 2 subinterfaces per Network Processor (NP) varies depending on the VLAN range values used. Ranges are programmed into a dedicated per-NP hardware region whose consumption depends on the specific start and end values of the range, so achievable sub-interface scale differs from one VLAN range to another.

Examples

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

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

Related Commands

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

encapsulation dot1q second-dot1q

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

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

Syntax Description

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

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Only one encapsulation command must be configured per service instance.

Examples

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

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

Related Commands

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

encapsulation untagged

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

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

Syntax Description

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

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

Example 1:

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

Example 2:

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

Related Commands

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

ethernet egress-filter

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

ethernet egress-filter strict

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration and Layer 2 subinterface configuration

Command History

Release	Modification
Release 3.7.3	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

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

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

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

ethernet filtering

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

ethernet filtering {**dot1ad** | **dot1q**}
no ethernet filtering

Syntax Description

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

Command Default

Ethernet filtering is not enabled.

Command Modes

interface configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

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

DA MAC Address	Description	dot1q	dot1ad
01-80-C2-00-00-00	STP, RSTP, MSTP, etc.	Discard	Data
01-80-C2-00-00-01	802.3X Pause Protocol	Discard	Discard
01-80-C2-00-00-02	Slow Protocols: 802.3ad LACP, 802.3ah OAM	Discard	Discard
01-80-C2-00-00-03	802.1X	Discard	Discard
01-80-C2-00-00-04	Reserved	Discard	Discard
01-80-C2-00-00-05	Reserved	Discard	Discard
01-80-C2-00-00-06	Reserved	Discard	Discard
01-80-C2-00-00-07	Reserved	Discard	Discard
01-80-C2-00-00-08	Provider Bridge Group Address (e.g. MSTP BPDU)	Discard	Discard
01-80-C2-00-00-09	Reserved	Discard	Discard

DA MAC Address	Description	dot1q	dot1ad
01-80-C2-00-00-0A	Reserved	Discard	Discard
01-80-C2-00-00-0B	Reserved	Discard	Data
01-80-C2-00-00-0C	Reserved	Discard	Data
01-80-C2-00-00-0D	Provider Bridge GVRP address	Discard	Data
01-80-C2-00-00-0E	802.1ab-LLDP	Discard	Data
01-80-C2-00-00-0F	Reserved	Discard	Data
01-80-C2-00-00-10	All Bridges address	Discard	Data
01-80-C2-00-00-20	GMRP / MMRP	Discard	Data
01-80-C2-00-00-21	GVRP / MVRP	Discard	Data
01-80-C2-00-00-22-2F	Other GARP addresses	Discard	Data
01-00-0C-CC-CC-CC	CDP, DTP, VTP, PaGP, UDLD	Discard	Data

Task ID

Task ID	Operations
interface	read, write

Examples

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

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#interface GigabitEthernet0/5/0/1
RP/0/RSP0/CPU0:router(config-if)#ethernet filtering dot1q
RP/0/RSP0/CPU0:router(config-if)#l2transport
RP/0/RSP0/CPU0:router(config-if-l2)#commit

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

```
 shutdown
!
interface GigabitEthernet0/5/0/6
 shutdown
!
interface GigabitEthernet0/5/0/7
 shutdown
RP/0/RSP0/CPU0:router#
```

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

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

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

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

ethernet source bypass egress-filter

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

ethernet source bypass egress-filter
no ethernet source bypass egress-filter

This command has no keywords or arguments.

Command Default

None

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

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

Related Commands

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

l2protocol (Ethernet)

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

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

Syntax Description

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

Command Default

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

Command Modes

Layer 2 transport configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
l2transport (Ethernet), on page 21	Enables Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode.

l2transport (Ethernet)

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

l2transport
no l2transport

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

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

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

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

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

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

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

Related Commands

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

local-traffic default encapsulation

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

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

Syntax Description

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

Command Default

Lowest numbered VLAN ID is chosen.

Command Modes

Subinterface configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

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

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

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

rewrite ingress tag

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

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

Syntax Description

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

Command Default

The frame is left intact on ingress.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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



Generic Routing Encapsulation Commands

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

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

- bandwidth, on page 28
- description (GRE), on page 29
- hw-module l3 feature gre-lite enable, on page 30
- ipv4 address, on page 31
- ipv4 mtu (LxVPN), on page 33
- ipv6 address (LxVPN), on page 34
- ipv6 mtu (LxVPN), on page 35
- keepalive, on page 36
- mtu (GRE), on page 37
- shutdown (GRE), on page 38
- tunnel destination, on page 39
- tunnel key, on page 40
- tunnel key-ignore, on page 42
- tunnel dfbit , on page 44
- tunnel mode, on page 45
- tunnel source, on page 46
- tunnel tos, on page 48
- tunnel ttl, on page 49
- tunnel vrf, on page 50

bandwidth

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

bandwidth *kbps*
no bandwidth *kbps*

Syntax Description

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

Command Default

None

Command Modes

interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
interface	read, write

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

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

description (GRE)

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

description *description-name*
no description

Syntax Description

description-name	Description of the Interface.

Command Default

None

Command Modes

Interface Configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
interface	read, write

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

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

hw-module l3 feature gre-lite enable

To enable the GRE lite mode, use the **hw-module l3 feature gre-lite enable** command in the configuration mode. To disable the feature, use the **no** form of this command.

hw-module l3 feature gre-lite enable

Syntax Description

hw-module l3 feature gre-lite enable	Enables the GRE lite mode.

Command Default

None

Command Modes

Interface Configuration

Command History

Release	Modification
Release 25.3.1	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.

Task ID

Task ID	Operation
interface	read, write

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

```
Router# configure
Router(config)# hw-module l3 feature gre-lite enable
Router(config)# Router# reload
Proceed with reload? [confirm]

Router(config)# interface tunnel-ip200
Router(config-if)# ipv4 unnumbered loopback100
Router(config-if)# tunnel mode gre ipv4 lite
Router(config-if)# tunnel source Loopback100
Router(config-if)# tunnel destination 10.10.10.1
Router(config-if)# commit
Router(config-if)# end
```

ipv4 address

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

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

Syntax Description

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

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read, write
acl	read, write

Examples

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

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

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

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

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

ipv4 mtu (LxVPN)

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

ipv4 mtu *size*
no ipv4 mtu *size*

Syntax Description

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

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read, write
acl	read, write

Examples

This example shows how to set the IPv4 MTU:

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

ipv6 address (LxVPN)

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

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

Syntax Description

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

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

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

Examples

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

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

ipv6 mtu (LxVPN)

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

ipv6 mtu *size*
no ipv6 mtu *size*

Syntax Description

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

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

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

Examples

This example shows how to set the IPv4 MTU:

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

keepalive

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

keepalive [*time_in_seconds* [*retry_num*]]
no keepalive

Syntax Description

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

Command Default

None

Command Modes

interface configuration

Command History

Usage Guidelines

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

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

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

mtu (GRE)

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

This is a Generic Routing Encapsulation (GRE) command.

mtu *size*
no mtu *size*

Syntax Description

size	Size of MTU in bytes. The default value is 1500.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
interface	read, write

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

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

shutdown (GRE)

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

This is a Generic Routing Encapsulation (GRE) command.

shutdown
no shutdown

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
interface	read, write

This example shows how to shut down a given interface:

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

tunnel destination

To specify a tunnel interface's destination 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

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

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

Related Commands

Command	Description
tunnel mode, on page 45	Configures the encapsulation mode of the tunnel interface.
tunnel source, on page 46	Sets a tunnel interface's source address.
tunnel tos, on page 48	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 49	Configures the Time-To-Live (TTL) for packets entering the tunnel.

tunnel key

To configure the key value for packets sent over a tunnel, use the **tunnel key** command. To delete the configured key value, use the **no** form of this command.

tunnel key *key-value*
no tunnel key *key-value*

Syntax Description

key-value	Specifies the tunnel key value. Range is from 0 to 4294967295.

Command Default

No value is configured.

Command Modes

interface 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.

- GRE tunnel key feature is supported only on Cisco ASR 9000 Enhanced Ethernet line cards. It is mandatory to have ingress and egress line cards as Enhanced Ethernet line cards.
- GRE tunnel keepalive is not supported with tunnel key. If the configuration for the GRE keepalives and tunnel key are present at the same time, the tunnel is brought down and a warning message is displayed.
- For a given router, either the same key or different keys can be configured under multiple GRE tunnels.
- Different traffic streams passing through the same GRE tunnel contain the same GRE key configured for that tunnel.

Task ID

Task ID	Operation
interface	read, write
tunnel	read, write

This example shows how to configure the tunnel key value at the GRE transmitter and receiver end:

```
!Local GRE Interface
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 10
RP/0/RSP0/CPU0:router(config-if)#ipv4 address 101.0.9.1 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# tunnel key 10
RP/0/RSP0/CPU0:router(config-if)# tunnel tos 96
RP/0/RSP0/CPU0:router(config-if)# tunnel source Loopback10
RP/0/RSP0/CPU0:router(config-if)# tunnel destination 33.0.9.33
```

```
!

!Remote GRE Interface

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 10
RP/0/RSP0/CPU0:router(config-if)#ipv4 address 101.0.9.2 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# tunnel key 10
RP/0/RSP0/CPU0:router(config-if)# tunnel tos 96
RP/0/RSP0/CPU0:router(config-if)# tunnel source Loopback10
RP/0/RSP0/CPU0:router(config-if)# tunnel destination 11.0.9.11

!
```

tunnel key-ignore

To ensure that the decapsulation router skips GRE key validation before accepting the packet, use the **tunnel key-ignore** command. To remove the tunnel key ignore feature, use the **no** form of this command.

tunnel key-ignore
no tunnel key-ignore

Syntax Description

This command has no keywords or arguments.

Command Default

Tunnel key-ignore is disabled.

Command Modes

interface 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.

Do not configure any key value under GRE tunnel that has tunnel key-ignore feature enabled. This is because the configured tunnel key overrides the tunnel key-ignore feature. As a result, packets that arrive with configured key value are accepted and undergo further processing at the decapsulation router, while the remaining packets without the key value are dropped.

Task ID

Task ID	Operation
interface	read, write
tunnel	read, write

This example shows how to configure the tunnel key-ignore feature at the GRE transmitter and receiver ends:

```
!Local GRE Interface
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 10
RP/0/RSP0/CPU0:router(config-if)#ipv4 address 101.0.9.1 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# tunnel key-ignore
RP/0/RSP0/CPU0:router(config-if)# tunnel tos 96
RP/0/RSP0/CPU0:router(config-if)# tunnel source Loopback10
RP/0/RSP0/CPU0:router(config-if)# tunnel destination 33.0.9.33
!

!Remote GRE Interface

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# interface tunnel-ip 10
```

```
RP/0/RSP0/CPU0:router#ipv4 address 101.0.9.2 255.255.255.0
RP/0/RSP0/CPU0:router# tunnel key-ignore
RP/0/RSP0/CPU0:router# tunnel tos 96
RP/0/RSP0/CPU0:router# tunnel source Loopback10
RP/0/RSP0/CPU0:router# tunnel destination 11.0.9.11

!
```

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

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

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

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

Related Commands

Command	Description
tunnel destination, on page 39	Specifies a tunnel interface's destination address.
tunnel mode, on page 45	Configures the encapsulation mode of the tunnel interface.
tunnel source, on page 46	Sets a tunnel interface's source address.
tunnel tos, on page 48	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 49	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

Syntax 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

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

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

Related Commands

Command	Description
tunnel destination, on page 39	Specifies a tunnel interface's destination address.
tunnel source, on page 46	Sets a tunnel interface's source address.
tunnel tos, on page 48	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 49	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

Usage Guidelines

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

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

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

Related Commands

Command	Description
tunnel destination, on page 39	Specifies a tunnel interface's destination address.
tunnel mode, on page 45	Configures the encapsulation mode of the tunnel interface.

Command	Description
tunnel tos, on page 48	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 49	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

Usage Guidelines

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

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

Related Commands

Command	Description
tunnel destination, on page 39	Specifies a tunnel interface's destination address.
tunnel mode, on page 45	Configures the encapsulation mode of the tunnel interface.
tunnel source, on page 46	Sets a tunnel interface's source address.
tunnel ttl, on page 49	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

Usage Guidelines

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

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

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure interface tunnel:

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

Related Commands

Command	Description
tunnel destination, on page 39	Specifies a tunnel interface's destination address.
tunnel mode, on page 45	Configures the encapsulation mode of the tunnel interface.
tunnel tos, on page 48	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel source, on page 46	Sets a tunnel interface's source address.

tunnel vrf

To specify the virtual routing and forwarding (VRF) instance of the interfaces of the tunnel endpoints, use the **tunnel vrf** command in tunnel interface configuration mode. To disassociate a VRF from the tunnel endpoints, use the **no** form of this command.

tunnel vrf *vrf-name*

Syntax Description

vrf-name	The name of the VRF instance.

Command Default

The tunnel addresses are looked up in the default VRF instance, that is, the global routing table.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
tunnel	read, write
interface	read, write

Example

The following example shows the tunnel "tunnel-ip1" endpoints associated with the VRF instance "blue".

```
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip1
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.3.3.3 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# keepalive 5 3
RP/0/RSP0/CPU0:router(config-if)# tunnel mode gre ipv4
RP/0/RSP0/CPU0:router(config-if)# tunnel source Loopback0
RP/0/RSP0/CPU0:router(config-if)# tunnel destination 10.5.5.5
RP/0/RSP0/CPU0:router(config-if)# tunnel vrf blue
```



Point to Point Layer 2 Services Commands

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

For detailed information about virtual private network concepts, configuration tasks, and examples, refer to the .

- advertise-mac, on page 54
- address-family l2vpn mspw, on page 55
- bgp, on page 56
- backup (L2VPN), on page 57
- backup disable (L2VPN), on page 59
- clear l2route evpn ipv4 , on page 61
- clear l2route evpn ipv6 , on page 62
- clear l2route evpn mac , on page 63
- clear l2vpn collaborators, on page 64
- clear l2vpn counters bridge mac-withdrawal, on page 65
- clear l2vpn forwarding counters, on page 66
- clear l2vpn forwarding counters bridge-domain mirp-lite, on page 67
- clear l2vpn forwarding message counters, on page 68
- clear l2vpn forwarding table, on page 69
- control-word, on page 70
- dynamic-arp-inspection, on page 71
- flood mode, on page 73
- generic-interface-list, on page 75
- global-id (L2VPN), on page 76
- interface (p2p), on page 77
- interworking ipv4, on page 78
- ipv4 source, on page 79
- l2tp static, on page 80
- ip-source-guard, on page 83
- l2transport, on page 85
- l2transport l2protocol, on page 87
- l2transport propagate, on page 89
- l2transport service-policy, on page 91
- l2vpn, on page 92

- l2vpn switchover, on page 93
- load-balancing flow, on page 94
- load-balancing flow-label, on page 95
- load-balancing pw-label, on page 97
- logging (l2vpn), on page 98
- logging nsr, on page 99
- monitor-session (l2vpn), on page 100
- mpls static label (L2VPN), on page 101
- neighbor (L2VPN), on page 103
- neighbor evpn, on page 105
- neighbor routed, on page 106
- nsr (L2VPN), on page 107
- option-b-asbr-only, on page 108
- pw-routing, on page 109
- preferred-path, on page 110
- protocol l2tpv3, on page 112
- pw-class (L2VPN), on page 113
- pw-class encapsulation l2tpv3, on page 114
- pw-class encapsulation mpls, on page 116
- pw-ether, on page 118
- pw-grouping, on page 120
- pw-iw, on page 121
- p2p, on page 122
- rd (L2VPN), on page 123
- sequencing (L2VPN), on page 125
- show bgp l2vpn evpn, on page 127
- show bgp l2vpn mspw, on page 129
- show bgp vrf-db, on page 130
- show evpn evi ead, on page 131
- show evpn internal-label, on page 133
- show dci-fabric-interconnect, on page 134
- show generic-interface-list , on page 137
- show l2tp session, on page 139
- show l2tp tunnel, on page 141
- show l2vpn, on page 143
- show l2vpn atom-db, on page 144
- show l2vpn collaborators, on page 147
- show l2vpn database, on page 149
- show l2vpn discovery, on page 152
- show l2vpn forwarding, on page 154
- show l2vpn forwarding message counters, on page 161
- show l2vpn generic-interface-list, on page 163
- show l2vpn index, on page 165
- show l2vpn nsr , on page 167
- show l2vpn process fsm, on page 169
- show l2vpn provision queue, on page 171

- show l2vpn pw-class, on page 173
- show l2vpn pwhe, on page 175
- show l2vpn resource, on page 177
- show l2vpn trace, on page 178
- show l2vpn xconnect, on page 180
- show tech-support l2vpn platform no-statistics, on page 189
- source (p2p), on page 191
- storm-control , on page 193
- switching-tlv (L2VPN), on page 196
- tag-impose, on page 198
- tos (l2vpn), on page 199
- transport mode (L2VPN), on page 201
- transport mode vlan passthrough, on page 203
- ttl (l2vpn), on page 204
- vpws-seamless-integration, on page 205
- xconnect group, on page 206

advertise-mac

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

advertise-mac

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EVPN

Command History

Release	Modification
Release 6.2.1	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.

The following example shows how to advertise local MAC.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 1
RP/0/RSP0/CPU0:router(config-evpn-evi)# bgp
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# table-policy spp-basic-6
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# route-target import 100:6005
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# route-target export 100:6005
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# exit
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac
```

address-family l2vpn mspw

To specify the L2VPN address family of the neighbor and to enter the address family configuration mode, use the **address-family l2vpn mspw** in the BGP configuration mode.

address-family l2vpn mspw

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

BGP configuration

Command History

Release	Modification
Release 5.1.2	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
bgp	read, write

The following example shows how to enter the address family configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router bgp 100
RP/0/RSP0/CPU0:router(config-bgp)# address-family l2vpn mspw
RP/0/RSP0/CPU0:router(config-bgp-af)#
```

bgp

To enable the BGP pseudowire routing capabilities and enter the bgp configuration submode, use the **bgp** command in the L2VPN routing configuration submode.

bgp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN routing configuration submode

Command History

Release	Modification
Release 5.1.2	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.

The following example shows how to enable BGP pseudowire routing capabilities.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router 2.2.2.2
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-routing
RP/0/RSP0/CPU0:router(config-l2vpn-pwr)# global-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-pwr)# bgp
RP/0/RSP0/CPU0:router(config-l2vpn-pwr-bgp)# rd 192.168.1.3:10
```

backup (L2VPN)

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN xconnect p2p pseudowire configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure backup pseudowires:

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

Related Commands

Command	Description
backup disable (L2VPN), on page 59	Specifies how long a backup pseudowire should wait before resuming operation after the primary pseudowire goes down.

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 103	Configures a pseudowire for a cross-connect.
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.
xconnect group, on page 206	Configures cross-connect groups.

backup disable (L2VPN)

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

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

Syntax Description

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

Command Default

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

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)#
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 103	Configures a pseudowire for a cross-connect.
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 113	Enters pseudowire class submode to define a pseudowire class template.
xconnect group, on page 206	Configures cross-connect groups.

clear l2route evpn ipv4

To clear either duplicate or frozen flags, or both, from EVPN MAC-IPv4 routes and re-enable local route learning for the corresponding IPv4 addresses, use **clear l2route evpn ipv4** command in EXEC mode.

clear l2route evpn ipv4 { *ipv4-address* } | **all** [**evi** *evi*] **frozen-flag**

Syntax Description

mac *mac-address*	Clears the route for the specified IPv4 address.
all	Clears all EVPN MAC-IPv4 routes that are marked as duplicate or permanently frozen.
evi *evi*	Clears EVPN MAC -IPv4 routes for the specified topology only.
frozen-flag	Clears either duplicate or frozen flag for the MAC-IPv4 routes that are identified by the specified options.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to clear duplicate or frozen flags, or both from EVPN MAC-IPv4 routes:

```
Router# clear l2route evpn ipv4 192.0.2.1 evi 1 frozen-flag
```

clear l2route evpn ipv6

To clear either duplicate or frozen flags, or both, from EVPN MAC-IPv6 routes and re-enable local route learning for the corresponding IPv6 addresses, use **clear l2route evpn ipv6** command in EXEC mode.

clear l2route evpn ipv6 {*ipv6-address*} | **all** [**evi** *evi*] **frozen-flag**

Syntax Description

mac *mac-address*	Clears the route for the specified IPv6 address.
all	Clears all EVPN MAC-IPv6 routes that are marked as duplicate or permanently frozen.
evi *evi*	Clears EVPN MAC-IPv6 routes for the specified topology only.
frozen-flag	Clear duplicate or frozen flag for the MAC-IPv6 routes that are identified by the specified options.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to clear either duplicate or frozen flags, or both, from EVPN MAC-IPv6 routes:

```
Router# clear l2route evpn IPv6 2001:DB8::1 evi 1 frozen-flag
```

clear l2route evpn mac

To clear either duplicate or frozen flags, or both, from EVPN MAC routes and re-enable local route learning for the corresponding MAC addresses, use **clear l2route evpn mac** command in EXEC mode.

clear l2route evpn mac {*mac-address*} | **all** [**evi** *evi*] **frozen-flag**

Syntax Description

mac *mac-address*	Clears the route for the specified MAC address.
all	Clears all EVPN MAC routes that are marked as duplicate or permanently frozen.
evi *evi*	Clears EVPN MAC routes for the specified topology only.
frozen-flag	Clears duplicate or frozen flag for the MAC routes that are identified by the specified options.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to clear duplicate or frozen flags, or both, from EVPN MAC routes:

```
Router# clear l2route evpn mac 0.12.3456 evi 1 frozen-flag
```

clear l2vpn collaborators

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

clear l2vpn collaborators

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
show l2vpn collaborators, on page 147	Displays information about the state of the interprocess communications connections between l2vpn_mgr and other processes.

clear l2vpn counters bridge mac-withdrawal

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

clear l2vpn forwarding counters

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

clear l2vpn forwarding counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to clear L2VPN forwarding counters:

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

clear l2vpn forwarding counters bridge-domain mirp-lite

To clear L2VPN forwarding MIRP counters, use the **clear l2vpn forwarding counters bridge-domain mirp-lite** command in EXEC mode.

clear l2vpn forwarding counters bridge-domain mirp-lite {**location** *node-id*}

Syntax Description

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

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, write, execute

This example shows how to clear all the MIRP counters:

```
RP/0/RSP0/CPU0:router# clear l2vpn forwarding counters bridge-domain mirp-lite location
0/1/CPU0
```

This example shows how to clear bridge-domain specific MIRP counters:

```
RP/0/RSP0/CPU0:router# clear l2vpn forwarding counters bridge-domain bg1:bd1 mirp-lite
location 0/1/CPU0
```

Related Commands

Command	Description
clear l2vpn forwarding counters, on page 66	Clears L2VPN forwarding counters.

clear l2vpn forwarding message counters

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

clear l2vpn forwarding message counters location *node-id*

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

clear l2vpn forwarding table

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

clear l2vpn forwarding table location *node-id*

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

control-word

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

control-word
no control-word

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN pseudowire class encapsulation configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

dynamic-arp-inspection

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

dynamic-arp-inspection {**logging** | **address-validation** {*src-macdst-macipv4*}}
no dynamic-arp-inspection {**logging** | **address-validation** {*src-macdst-macipv4*}}

Syntax Description

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

Command Default

Dynamic ARP inspection is disabled.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

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

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

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

flood mode

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

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

Syntax Description

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

Command Default

The bridge domain operates in the Bandwidth Optimized Mode.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The **flood mode** command allows you to change the flood optimization mode to either Convergence Optimized mode or Resilience Optimized mode.

- Convergence Optimized mode floods all traffic to all line cards; all unknown unicast packets, all broadcast packets, and all multicast packets are flooded over all other bridge domain network interfaces.
- Resilience Optimized mode works like Bandwidth Optimized mode, except that it floods traffic to both primary and backup FRR links for a Pseudowire.

Changing the bridge domain flood mode requires removing and reconfiguring the bridge domain.

To avoid the loss of BUM traffic over L2 service when L3 FRR is triggered, configure **flood mode resilience optimized** command under L2VPN.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.

generic-interface-list

To configure generic interface list, use the **generic-interface-list** command in global configuration mode.

generic-interface-list *list-name*

Syntax Description

list-name	Name of the interface list.

Command Default

None

Command Modes

Global 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
l2vpn	read, write

Example

This example shows how to configure generic interface list:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# generic-interface-list interfacelist1
RP/0/RSP0/CPU0:router(config-if-list)# interface GigabitEthernet 0/2/0/1
RP/0/RSP0/CPU0:router(config-if-list)# interface GigabitEthernet 0/3/0/1
RP/0/RSP0/CPU0:router(config-if-list)# exit
```

Related Commands

Command	Description
show l2vpn generic-interface-list, on page 163	Displays all the L2VPN virtual interfaces.

global-id (L2VPN)

To configure the L2VPN global ID value for the router, use the **global-id** command in the L2VPN routing configuration submode.

global-id *value*

Syntax Description

value	Specifies the global-id value. Range is from 1 to 4294967295.

Command Default

If BGP is used as the redistribution L2 protocol, then the default value is the BGP AS number. Otherwise, the default value is 0.

Command Modes

L2VPN routing configuration submode

Command History

Release	Modification
Release 5.1.2	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.

This command overwrites the AS number from BGP.

Task ID

Task ID	Operation
l2vpn	read, write

The following example shows how to configure L2VPN global ID value:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#router-id 2.2.2.2
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-routing
RP/0/RSP0/CPU0:router(config-l2vpn-pwr)# global-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-pwr)# bgp
RP/0/RSP0/CPU0:router(config-l2vpn-pwr-bgp)# rd 192.168.1.3:10
```

interface (p2p)

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

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

Syntax Description

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

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.

interworking ipv4

To configure IPv4 interworking, use the **interworking ipv4** command in the p2p configuration submode. To return to the default behavior, use the **no** form of this command.

interworking ipv4
no interworking ipv4

Syntax Description

ipv4	Sets IPv4 interworking.

Command Default

None

Command Modes

p2p configuration submode

Command History

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group gr1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p gr1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interworking ipv4
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)#
```

Related Commands

Command	Description
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.

ipv4 source

To configure source IP address for the pseudowire class with encapsulation mpls, use the **ipv4 source** command in the L2VPN pseudowire class encapsulation mpls configuration mode.

ipv4 source *source-ip-address*

Syntax Description

source-ip-address	Source IP address.

Command Default

None

Command Modes

L2VPN pseudowire class encapsulation mpls configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to configure the source ip address:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#pw-class kant1
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)#encapsulation mpls
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)#ipv4 source 112.22.1.4
```

Related Commands

Command	Description
pw-class encapsulation mpls, on page 116	Configures MPLS pseudowire encapsulation.

l2tp static

To enable the Layer 2 Tunneling Protocol (L2TP) static submode, and perform L2TP pseudowire configurations, use the **l2tp static** command in p2p pseudowire configuration submode. To disable the L2TP static submode, use the **no** form of this command.

l2tp static [**local** {**cookie** {**secondary size** | **size**} {**0** | **4** | **8**} **value** *value* | **session** *session id*} | **remote** {**cookie size** {**0** | **4** | **8**} **value** *value* | **session** *session id*}]
no l2tp static [**local** {**cookie** {**secondary size** | **size**} {**0** | **4** | **8**} **value** *cookie value* | **session** *session id*} | **remote** {**cookie size** {**0** | **4** | **8**} **value** *cookie value* | **session** *session id*}]

Syntax Description

local	(Optional) Configures local cookies and sessions.
cookie	Sets L2TP pseudowire static local or remote cookie.
secondary size	Sets L2TP pseudowire static local cookie secondary size.
size	Sets L2TP pseudowire static local cookie size.
value	Sets the value of the cookie.
cookie value	Value of the cookie. The cookie values are specified based on the configured cookie size: • Cookie size 0—No cookie value is set. • Cookie size 4—Lower 4 bytes value (<0x0-0xffffffff>) is set. • Cookie size 8—Lower 4 bytes value and higher 4 bytes values (<0x0-0xffffffff> <0x0-0xffffffff>) are set.
session	Sets L2TP pseudowire static local or remote session.
session id	Session ID. Range is from 1 to 65535.
remote	(Optional) Configures remote cookies and sessions.

Command Default

None

Command Modes

p2p pseudowire 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.

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to enter the l2tp static configuration sub mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static
```

This example shows how to configure local and remote session-id:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static local session 1
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static remote session 1
```

This example shows how to configure cookie size and values:

This example is with cookie size 0:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static local cookie size 0
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static remote cookie size 0
```

This example is with cookie size 4:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static local cookie size 4 value
<0x0-0xffffffff>
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static remote cookie size 4 value
<0x0-0xffffffff>
```

This example is with cookie size 8 (lower 4 bytes entered first and then higher 4 bytes):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static local cookie size 8 value
<0x0-0xffffffff> <0x0-0xffffffff>
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static remote cookie size 8 value
<0x0-0xffffffff> <0x0-0xffffffff>
```

This example show how to configure a secondary local cookie:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn xconnect group l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static local cookie secondary size 8 value
<0x0-0xffffffff> <0x0-0xffffffff>
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.
xconnect group, on page 206	Configures cross-connect groups.
neighbor (L2VPN), on page 103	Configures a pseudowire for a cross-connect.

ip-source-guard

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

ip-source-guard logging
no ip-source-guard logging

Syntax Description

logging	(Optional) Enables logging.

Command Default

IP Source Guard is disabled.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 4.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

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

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

l2transport

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

l2transport
no l2transport

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The l2transport command and these configuration items are mutually exclusive:

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

Ethernet Port Mode:

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

Ethernet VLAN Mode:

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

Ethernet VLAN Mode (QinQ):

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

Ethernet VLAN Mode (QinAny):

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

l2transport l2protocol

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

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

Syntax Description

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

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

These L2 protocols are available:

- Cisco Discovery Protocol (CDP)—CDP is protocol-independent and is used to obtain protocol addresses, platform information, and other data about neighboring devices.
- PVST maintains a spanning tree instance for each VLAN configured in the network and permits a VLAN trunk to be forwarding for some VLANs and not for others. It can also load balance Layer 2 traffic by forwarding some VLANs on one trunk and other VLANs n others.

- Spanning-Tree Protocol (STP)—STP is a link management protocol that provides path redundancy in the network. For Ethernet networks to function properly, only one active path can exist between two stations.
- VLAN Trunk Protocol (VTP)—VTP is a Cisco-proprietary protocol that reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain.

Task ID

Task ID	Operations
l2vpn	read, write
atm	read, write

Examples

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

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

l2transport propagate

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

l2transport propagate remote-status
no l2transport propagate remote-status

Syntax Description

remote-status	Propagates remote link status changes.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Note If you configure the propagate Layer 2 transport using this command on both ends of the PW (head and tail end), the PW might flap continuously. Use the **carrier-delay** command on the attachment circuit to stabilize the PW.

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

l2transport service-policy

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

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

Syntax Description

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

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write
atm	read, write

Examples

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

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

l2vpn

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

l2vpn
no l2vpn

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enter L2VPN configuration mode:

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

l2vpn switchover

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write, execute

Examples

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

```
RP/0/RSP0/CPU0:router# l2vpn switchover xconnect neighbor 10.1.1.1 pw-id 2
```

Related Commands

Command	Description
backup disable (L2VPN), on page 59	Specifies how long a backup pseudowire should wait before resuming operation after the primary pseudowire goes down.

load-balancing flow

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

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

Syntax Description

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

Command Default

The default load balancing is based on the source and destination MAC addresses.

Command Modes

L2VPN configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to set the L3 flow based load balancing:

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

load-balancing flow-label

To balance the load based on flow-labels, use the **load-balancing flow label** command in 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** | **receive** | **transmit**}[**static**]
no load-balancing flow-label {**both** | **receive** | **transmit**}[**static**]

Syntax Description

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

Command Default

None

Command Modes

L2vpn pseudowire class mpls configuration 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 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

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

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

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

Related Commands

Command	Description
pw-class encapsulation mpls, on page 116	Configures MPLS pseudowire encapsulation.

load-balancing pw-label

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

load-balancing pw-label

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Pseudowire class configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to set the bridge ID:

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

logging (l2vpn)

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

logging pseudowire status
no logging pseudowire status

Syntax Description

pseudowire status	Enables pseudowire state change logging.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
l2vpn, on page 92	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
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.

monitor-session (l2vpn)

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

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

Syntax Description

session-name	Name of the monitor session to configure.

Command Default

No default behavior or values

Command Modes

Point-to-point cross connect configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
See the **monitor session** command in the *Interface and Hardware Component Command Reference for Cisco ASR 9000 Series 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* }

Syntax Description

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

Command Default

The default behavior is a dynamic label assignment.

Command Modes

L2VPN cross-connect P2P pseudowire configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
Router# configure
Router(config)# l2vpn xconnect group l2vpn
Router(config-l2vpn-xc)# p2p rtrA_to_rtrB
Router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
Router(config-l2vpn-xc-p2p-pw)# mpls static label local 800 remote 500
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
neighbor (L2VPN), on page 103	Configures a pseudowire for a cross-connect.
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.

Command	Description
xconnect group, on page 206	Configures cross-connect groups.

neighbor (L2VPN)

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

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

Syntax Description

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

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

A cross-connect may have two segments:

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



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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 113	Enters pseudowire class submode to define a pseudowire class template.
xconnect group, on page 206	Configures cross-connect groups.

neighbor evpn

To enable EVPN-VPWS endpoint on the p2p cross-connect, use the **neighbor evpn** command in the p2p configuration submode.

neighbor evpn evi *vpn-id***target** *ac-id*

Syntax Description

evi	*vpn-id*	Virtual Private Network Identifier where this p2p xconnect is setup.
target	*ac-id*	Specifies the targeted remote attachment circuit id of the EVPN.

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 6.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

The following example shows how to enable EVPN-VPWS endpoint on the p2p cross-connect.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:routerRP/0/RP00RSP0/CPU0:router# interface TenGigE0/1/0/12
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group xc1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p vpws
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# neighbor evpn evi 100 target 80
```

neighbor routed

To enable pseudowire routing configuration submode for the p2p cross-connect, use the **neighbor routed** command in the p2p configuration submode.

neighbor routed *global-id*:*prefix*:*ac-id* **source** *ac-id*

Syntax Description

global-id	Targeted remote autonomous system number.
prefix	Targeted remote PE IP address.
ac-id	Specifies the targeted remote attachment circuit id.
source *ac-id*	Specifies the local attachment circuit ID.

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 5.1.2	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
l2vpn	read, write

The following example shows how to enable pseudowire routing configuration submode for the p2p cross-connect.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group pw-he1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p pw-ss
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# neighbor routed 100:2.2.2.2:10 source 10
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pwr)# pw-class dynamic_sspw
```

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

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

Note NSR is enabled by default for L2VPN On Cisco IOS XR 64 bit operating system. You cannot configure the **nsr** command under L2VPN configuration submode.

Task ID

Task ID	Operation
l2vpn	read, write

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.

option-b-asbr-only

To enter option-b-asbr-only configuration mode, use the **option-b-asbr-only** command under the address-family L2VPN EVPN global configuration mode.

option-b-asbr-only

Syntax Description

option-b-asbr-only	Enables Inter-AS option-B for L2VPN EVPN address-family identifier (AFI) and subsequent address-family identifier (SAFI).

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

This example shows how to enable the ASBR router for option-B label exchange:

```
Router(config)# router bgp 300
Router(config-bgp)# address-family l2vpn evpn
Router(config-bgp-af)# option-b-asbr-only
Router(config-evpn-instance)# commit
```

pw-routing

To enable pseudowire routing capabilities and enter the pseudowire routing configuration submode, use the **pw-routing** command in the L2VPN routing configuration submode.

pw-routing

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

L2VPN routing configuration submode

Command History

Release	Modification
Release 5.1.2	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
l2vpn	read, write

The following example shows how to enable pseudowire routing capabilities:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#router-id 2.2.2.2
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-routing
RP/0/RSP0/CPU0:router(config-l2vpn-pwr)# global-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-pwr)# bgp
RP/0/RSP0/CPU0:router(config-l2vpn-pwr-bgp)# rd 192.168.1.3:10
```

preferred-path

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

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

Syntax Description

interface	Interface for the preferred path.
tunnel-ip	IP tunnel interface name for the preferred path.
value	Tunnel number for preferred path.
tunnel te	Specifies the TE tunnel interface name for the preferred path.

Command Default

None

Command Modes

Encapsulation MPLS configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to configure preferred-path tunnel settings:

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

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

Related Commands

Command	Description
show l2vpn xconnect, on page 180	Displays brief information on configured cross-connects.

protocol l2tpv3

To configure Layer 2 Tunneling Protocol Version 3 (L2TPv3) as the signaling protocol for a pseudowire class, use the **protocol l2tpv3** command in L2VPN pseudowire class encapsulation L2TPv3 configuration mode. To disable L2TPv3 as the signaling protocol for a pseudowire class, use the **no** form of this command.

protocol l2tpv3[**class** *class_name*]
no protocol l2tpv3[**class** *class_name*]

Syntax Description

class	Specifies the L2TPv3 class.
class_name	The L2TPv3 class name.

Command Default

None

Command Modes

L2VPN pseudowire class encapsulation L2TPv3 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	Operation
l2vpn	read, write

Example

This example shows how to set the encapsulation and protocol to L2TPv3:

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

pw-class (L2VPN)

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

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

Syntax Description

class-name	Pseudowire class name.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.

pw-class encapsulation l2tpv3

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to define L2TPV3 pseudowire encapsulation:

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

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

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

Related Commands

Command	Description
pw-class (L2VPN), on page 113	Enters pseudowire class submode to define a pseudowire class template.
pw-class encapsulation mpls, on page 116	Configures MPLS pseudowire encapsulation.

pw-class encapsulation mpls

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

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

Syntax Description

class-name	Encapsulation class name.
control word	Disables control word for MPLS encapsulation. Disabled by default.
ipv4	Sets the local source IPv4 address.
load-balancing	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.
switching tlv	Configures switching TLV to be hidden or not.
tag-rewrite	Configures VLAN tag rewrite.
transport-mode	Configures transport mode to be either Ethernet or VLAN.
vccv none	Enables or disables the VCCV verification type.

Command Default

None

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Release	Modification
Release 3.9.0	The following keywords were added: • **preferred-path** • **sequencing** • **switching tlv** • **tag-rewrite** • **transport-mode**

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to define MPLS pseudowire encapsulation:

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

Related Commands

Command	Description
pw-class (L2VPN), on page 113	Enters pseudowire class submode to define a pseudowire class template.

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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface pw-ether 78
RP/0/RSP0/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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group xc1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)#p2p grp1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)#interface pw-ether 78
```

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

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

```
RP/0/RSP0/CPU0:router(config)# interface pw-ether 78
RP/0/RSP0/CPU0:router(config-if)# l2overhead 32
```

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface pw-ether 78
RP/0/RSP0/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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface pw-ether 78
RP/0/RSP0/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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface pw-ether 78
RP/0/RSP0/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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface pw-ether 78
RP/0/RSP0/CPU0:router(config-if)# mtu 128
```

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface pw-ether 78
RP/0/RSP0/CPU0:router(config-if)# bandwidth 256
```

Related Commands

Command	Description
p2p, on page 122	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
l2vpn	read, write

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
show l2vpn, on page 143	Displays L2VPN information

pw-iw

To configure a PWHE IP Interworking interface, use the **pw-iw** command in p2p configuration submode. To return to the default behavior, use the **no** form of this command.

pw-iw *value*
no pw-iw *value*

Syntax Description

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

Command Default

None

Command Modes

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
l2vpn	read, write

This example shows the sample output of a PWHE IP interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group xc1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)#p2p grp1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)#interface pw-iw 78
```

Related Commands

Command	Description
pw-ether, on page 118	Configures a Pseudowire Headend (PWHE) Ethernet interface.

p2p

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN xconnect

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
interface (p2p), on page 77	Configures an attachment circuit.

rd (L2VPN)

To configure BGP route distinguisher, use the **rd** command in the L2VPN pseudowire routing bgp configuration submode or the L2VPN bridge domain VFI autodiscovery bgp submode or the L2VPN cross-connect mp2mp autodiscovery bgp sub-mode, as applicable.

rd {*ASN* **:** *index* | *ipv4-address* **:** *index*}

Syntax Description

ASN	Specifies the 2-byte or 4-byte autonomous system number.
index	Specifies the index value. If the ASN is 2-byte, then the index value is 4-byte. If the ASN is 4-byte or the index is preceded by an IPv4 address, then the index value is 2-byte.
ipv4-address	Indicates the IP address (4 bytes). The index value associated with the IP address is 2-byte.

Command Default

Default value is auto-generated in the format IPv4 address : nn; where, IPv4 address is set to the BGP router-id for all features or to L2VPN router-id for pseudowire routing only, and nn is the index value that is auto-generated.

Command Modes

L2VPN pseudowire routing BGP configuration submode

L2VPN bridge domain VFI autodiscovery BGP submode

L2VPN cross-connect mp2mp autodiscovery BGP submode

Command History

Release	Modification
Release 3.7.2	This command is introduced for the L2VPN bridge domain VFI autodiscovery BGP and L2VPN cross-connect mp2mp autodiscovery BGP submodes.
Release 5.1.2	This command is introduced for the L2VPN pseudowire routing BGP configuration submode.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

The following example shows how to configure BGP route distinguisher.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#router-id 2.2.2.2
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-routing
RP/0/RSP0/CPU0:router(config-l2vpn-pwr)# global-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-pwr)# bgp
RP/0/RSP0/CPU0:router(config-l2vpn-pwr-bgp)# rd 192.168.1.3:10
```

sequencing (L2VPN)

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN pseudowire class encapsulation mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
pw-class (L2VPN), on page 113	Enters pseudowire class submode to define a pseudowire class template.

show bgp l2vpn evpn

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 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
bgp	read

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

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

show bgp l2vpn mspw

To display the information about L2VPN single-segment pseudowires, use the **show bgp l2vpn mspw** command in the EXEC mode.

show bgp l2vpn mspw

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.1.2	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
bgp	read

The following example displays the information about L2VPN Single-Segment Pseudowires

```
RP/0/0/CPU0:PE2#show bgp l2vpn mspw
Mon Apr 13 16:27:18.878 PDT
BGP router identifier 200.200.200.200, local AS number 100
BGP generic scan interval 100 secs
BGP table state: Active
Table ID: 0x0   RD version: 14
BGP main routing table version 5
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 4.3.2.1:0
*> [100][200.200.200.200]/64
                      0.0.0.0                                  0 i
Route Distinguisher: 4.3.2.1:1
*> [100][100.100.100.100][200]/96
                      10.10.10.2
```

show bgp vrf-db

To display the BGP VRF database information, use the **show bgp vrf-db** command in the EXEC mode.

show bgp vfr-db {**all** *vrf table id*}

Syntax Description

all	Displays all BGP VRF database table information.
vrf table id	Displays the BGP VRF database information for the specific VRF table ID.

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
l2vpn	read

Example

This sample output shows the BGP VRF database information with the VRF table ID filter:

```
#show bgp vrf-db table 0x00000001
Tue Jun 14 14:39:32.468 EDT

VRF-TBL: bd1 (L2VPN EVPN)
  TBL ID: 0x00000001
  RSI Handle: 0x0
  Refcount: 24
  Import:
    RT-List: RT:100:1
    Stitching RT-List: RT:101:1
  Export:
    RT-List: RT:100:1
    Stitching RT-List: RT:101:1
```

show evpn evi ead

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

show evpn evi ead detail

Syntax Description

evi	Specifies the EVPN Instance Identifier. This is used to derive the default Route Distinguisher and Route Targets.
ead	Specifies the EVPN ead routes.
detail	Displays detailed information.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 6.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN EVI detailed information:

```
RP/0/RSP0/CPU0:router#show evpn evi ead detail
Mon Apr 18 13:19:44.311 EDT

EVI   Ethernet Segment Id      EtherTag Nexthop                                Label
----- ----------------------- -------- ------------------------------------- --------
1     00a1.a2a3.a4a5.a6a7.a8a9 0        ::                                    24006
                                       2.2.2.2                               24007
   Source: Local, Remote, MPLS, VXLAN
1     00a1.a2a3.a4a5.a6a7.a8a9 ffffffff 2.2.2.2                               0
   Source: Remote, Unknown encap
200   0000.0000.0000.0000.0000 1        ::                                    24025
   Source: Local, MPLS
200   0000.0000.0000.0000.0000 4        ::                                    24026
   Source: Local, MPLS
200   0000.0000.0000.0000.0000 11       ::                                    24027
   Source: Local, MPLS
```

```
300   00a1.a2a3.a4a5.a6a7.a8a9 0        ::                                      24004
                                        2.2.2.2                                 24005
   Source: Local, Remote, MPLS, VXLAN
300   00a1.a2a3.a4a5.a6a7.a8a9 ffffffff 2.2.2.2                                 0
   Source: Remote, Unknown encap
302   00a1.a2a3.a4a5.a6a7.a8a9 0        ::                                      24008
   Source: Local, MPLS, VXLAN
400   00b1.b2b3.b4b5.b6b7.b8b9 0        ::                                      24010
   Source: Local, MPLS
```

Related Commands

Command	Description
evpn, on page 341	Enters EVPN configuration mode.
evpn evi, on page 342	

show evpn internal-label

To display EVPN internal label associated configuration information, use the **show evpn internal-label** command in the EXEC mode.

show evpn internal-label [**vpn-id** *evi* [**detail**]]

Syntax Description

vpn-id *evi*	Displays information for a specified E-VPN Identifier.
detail	Displays detailed 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
l2vpn	read

Example

This sample output shows the EVPN internal label associated configuration information.

```
show evpn internal-label vpn-id 1 detail
Tue Jun 14 16:18:51.563 EDT

EVI   Ethernet Segment Id                      EtherTag Label
----- ---------------------------------------- -------- --------
1     0088.0000.0000.0000.0001                 0        24036
   Multi-paths resolved: TRUE
   Multi-paths local label: 24036
   Pathlists:
      MAC     1 entries
      EAD/ES  203.0.113.1                              0
              209.165.200.225                          0
      EAD/EVI 203.0.113.1                              24001
              209.165.200.225                          24001
      Summary 203.0.113.1                              24001
              209.165.200.225                          24001
```

show dci-fabric-interconnect

To display the DCI fabric tenant interconnect information, use the **show dci-fabric-interconnect** command in the EXEC mode.

show dci-fabric-interconnect {**auto-configuration-pools** | **dci-vrf-db** [**vrf** *vrfname*] | **fabric** [*fabric id* | **opflex-session**] | **fabric-vrf-db** [**fabric** *fabric id*]}

Syntax Description

auto-configuration-pools	Displays auto configuration pool parameters.
dci-vrf-db	Displays DCI VRF database information.
vrf *vrf name*	Displays DCI VRF database for a specific VRF.
fabric *fabric id*	Displays fabric information for fabric ID. The range is from 1000 to 9999.
opflex-session	Displays opflex session information.
fabric-vrf-db	Displays fabric VRF database information.
fabric *fabric id*	Displays fabric VRF database for a fabric ID.

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
l2vpn	read

Example

This sample output shows the DCI fabric interconnect information with the auto-configuration-pools filter:

```
RP/0/RSP0/CPU0:router# show dci-fabric-interconnect auto-configuration-pools
Sat May 28 08:12:24.192 PDT
Auto Configuration Pool Info
-------------------------------------------------
Pool:Min-Max          Used Num Bits    Used Range
-------------------------------------------------
```

```
VNI-Pool:0001-1000    Used:10          Used:1-10
BD-Pool :0001-1000    Used:10          Used:1-10
BVI-Pool:0001-1000    Used:10          Used:1-10
-------------------------------------------------
```

Example

This sample output shows the DCI fabric interconnect information with the fabric opflex-session filter:

```
RP/0/RSP0/CPU0:router# show dci-fabric-interconnect fabric opflex-session
Sat May 28 08:12:09.326 PDT
Fabric Id: 1000
State: Config Complete(Sat May 28 08:09:01.813 PDT)
       Active (Healthy)(Wed Dec 31 16:00:00.000 PST)

Peers:
Peer-IP            Peer-Port    Peer-Status /Timestamp
===============    =========    ========================================
209.165.200.225    8009         Ready     /(Wed Dec 31 16:00:01.000 PST)
================================================================================
```

Example

This sample output shows the DCI fabric interconnect information with the fabric-vrf-db filter:

```
RP/0/RSP0/CPU0:router# show dci-fabric-interconnect fabric-vrf-db
Tue Jul 26 16:13:30.101 PDT
Flags: S = STALE
--------------------------------------------------------------------------------
Fabric Id: 1000  Number of VRFs: 0010
--------------------------------------------------------------------------------
Fabric-VRF:FV1000_2  DCI VRF:DV2  Flags:
         v4 Import RTs:(100:19333144)
         v4 Export RTs:(100:19333144)
         v6 Import RTs:(100:19333144)
         v6 Export RTs:(100:19333144)

Fabric-VRF:FV1000_3  DCI VRF:DV3  Flags:
         v4 Import RTs:(100:19333144)
         v4 Export RTs:(100:19333144)
         v6 Import RTs:(100:19333144)
         v6 Export RTs:(100:19333144)

Fabric-VRF:FV1000_4  DCI VRF:DV4  Flags:
         v4 Import RTs:(100:19333144)
         v4 Export RTs:(100:19333144)
         v6 Import RTs:(100:19333144)
         v6 Export RTs:(100:19333144)

Fabric-VRF:FV1000_5  DCI VRF:DV5  Flags:
         v4 Import RTs:(100:19333144)
         v4 Export RTs:(100:19333144)
         v6 Import RTs:(100:19333144)
         v6 Export RTs:(100:19333144)
```

Example

This sample output shows the DCI fabric interconnect information with the dci-vrf-db filter:

```
RP/0/RSP0/CPU0:router# show  dci-fabric-interconnect dci-vrf-db
Sat May 28 08:12:17.401 PDT
Flags: AP = ADD_PENDING, DP = DELETE_PENDING, C = CONFIG_APPLIED, S = STALE
------------------------------------------------------------------------------
DCI VRF:DV6  Flags:C
         Number of Fabric VRFs: 0002
         Fabric VRFs: (1000,FV1000_6); (2000,FV2000_6)
         v4 RT: (Import:1000:1000, Export:         )/Flags:C
                (Import:1000:2000, Export:         )/Flags:C
         v6 RT: (Import:2000:1000, Export:         )/Flags:C
                (Import:2000:2000, Export:         )/Flags:C
         VNI Id:0007 ; BD-Name:fti-bd-7
         BVI-ID:0007 ; BVI-IP:169.254.1.30 ; BVI-IPV6: Enabled
------------------------------------------------------------------------------
DCI VRF:DV7  Flags:C
         Number of Fabric VRFs: 0002
         Fabric VRFs: (1000,FV1000_7); (2000,FV2000_7)
         v4 RT: (Import:1000:1000, Export:         )/Flags:C
                (Import:1000:2000, Export:         )/Flags:C
         v6 RT: (Import:2000:1000, Export:         )/Flags:C
                (Import:2000:2000, Export:         )/Flags:C
         VNI Id:0008 ; BD-Name:fti-bd-8
         BVI-ID:0008 ; BVI-IP:169.254.1.30 ; BVI-IPV6: Enabled
------------------------------------------------------------------------------
```

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
l2vpn	read

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

```
RP/0/RSP0/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/RSP0/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/RSP0/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
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.

show l2tp session

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Usage Guidelines

To use this command, you must be in a user group associated with a task 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-l2vpn-pw)# show l2tp session brief
Tue Jun 10 12:51:30.901 UTC
LocID      TunID      Peer-address    State     Username, Intf/sess/cir  Vcid, Circuit

1606803058 1487464659 26.26.26.26     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 1: show l2tp session brief Field Descriptions

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

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

```
RP/0/RP00/CPU0:router(config-l2vpn-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
```

Related Commands

Command	Description
#unique_113	

show l2tp tunnel

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-encap-mpls)# show l2tp 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 2: show l2tp tunnel Field Descriptions

Field	Description
LocTunID	Local session ID.
RemTunID	Remote session ID.

Field	Description
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/RSP0/CPU0:router(config-l2vpn-encap-mpls)# show l2tp 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
```

Related Commands

Command	Description
show l2tp session, on page 139	Displays information about L2TP sessions.

show l2vpn

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

show l2vpn

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
l2vpn	read

Example

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
pw-grouping, on page 120	Enables Pseudowire Grouping

show l2vpn atom-db

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

show l2vpn atom-db [**detail** | **l2-rid** | **ldp-rid** | **local-gid** | **neighbor** | **preferred-path** | **remote-gid** | **source**]

Syntax Description

detail	Specifies the details of the database.
l2-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 10.0.0.1** command:

```
RP/0/RSP0/CPU0:router# show l2vpn atom-db source 10.0.0.1
Peer ID         Source         VC ID      Encap    Signaling   FEC     Discovery
172.16.0.1         10.0.0.1       1          MPLS     LDP         128     none
```

This example shows the sample output of the **show l2vpn atom-db source 10.0.0.1 detail** command:

```
RP/0/RSP0/CPU0:router# show l2vpn atom-db source 10.0.0.1 detail
  PW: neighbor 172.16.0.1, PW ID 1, state is down ( provisioned )
```

```
PW class class1, XC ID 0x1
Encapsulation MPLS, protocol LDP
Source address 10.0.0.1
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

  MPLS         Local                          Remote
  ------------ ------------------------------ ------------------------------
  Label        16000                          unknown
  Group ID     0x20000060                     0x0
  Interface    GigabitEthernet0/0/0/1.1       unknown
  MTU          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 = 172.16.0.1, 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
  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]
 ----------------------------------------
 Time                Event                          Value
 ====                =====                          ==========
 12/13/2010 15:28:26 LSP Down                       0
 12/13/2010 15:28:26 Provision                      0
 12/13/2010 15:28:26 LSP Down                       0
 12/13/2010 15:28:26 Connect Req                    0
 12/13/2010 15:28:26 Rewrite create                 0x100000
 12/13/2010 15:28:26 Got label                      0x3e80
 12/13/2010 15:28:26 Local Mtu                      0x5e0
12/13/2010 15:28:26 Peer Up                        0
```

show l2vpn collaborators

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

show l2vpn collaborators

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

This table describes the significant fields shown in the display.

Table 3: show l2vpn collaborators Field Descriptions

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

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

Related Commands

Command	Description
clear l2vpn collaborators, on page 64	Clears the state change counters for L2VPN collaborators.

show l2vpn database

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

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
l2vpn	read

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

```
RP/0/RSP0/CPU0:router# show l2vpn 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/l2-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/l2-mtu: 1504/1518
```

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

```
RP/0/RSP0/CPU0:router# show l2vpn database node
    0/RSP0/CPU0
        MA: vlan_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             2               0


        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             0               0



    0/0/CPU0
        MA: vlan_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 15:00:40 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 l2vpn discovery

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

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

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

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

Related Commands

Command	Description
show l2vpn bridge-domain (VPLS), on page 283	Display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains.

show l2vpn forwarding

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

show l2vpn forwarding {**xconnect** | **bridge-domain** | **counter** | **detail** | **hardware** | **inconsistent** | **interface** | **l2tp** | **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.
l2tp	Displays L2TPv3 related forwarding information.
location *node-id*	Displays layer2_fib manager information for the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.
message	Displays messages exchanged with collaborators.
mstp	Displays multi-spanning tree related forwarding information.
resource	Displays resource availability information in the layer2_fib manager.
retry-list	Displays retry list related information.

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Task ID

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


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

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

RP/0/RSP0/CPU0:router#show l2vpn forwarding bridge-domain detail location 0/2/CPU0
Bridge-domain name: bg1:bd1, id: 0, state: up
….
GigabitEthernet0/2/0/0.4, state: oper up
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/RSP0/CPU0:router# show l2vpn forwarding counter location 0/7/CPU0
Legend: ST = State, DN = Down

Segment 1                              Segment 2           ST     Byte
                                                                                Switched
------------------------------ ----------------------    --      ---------
pw-span-test (Monitor-Session) mpls  172.16.0.1  UP       0


RP/0/RSP0/CPU0:router #Show l2vpn forwarding monitor-session location 0/7/CPU0
Segment 1                            Segment 2                              State
------------------------------------ -------------------------------------- ------
pw-span-test(monitor-session)  mpls    172.16.0.1                      UP
pw-span-sess(monitor-session)  mpls    192.168.0.1                      UP


RP/0/RSP0/CPU0:router #Show l2vpn forwarding monitor-session pw-span-test location 0/7/CPU0
Segment 1                               Segment 2                             State
------------------------------------ -------------------------------------- ------
pw-span-test(Monitor-Session) mpls    172.16.0.1                     UP


Example 4:
RP/0/RSP0/CPU0:router #show l2vpn forwarding detail location 0/7/CPU0
  Xconnect id: 0xc000001, Status: up
  Segment 1
    Monitor-Session, pw-span-test, status: Bound
  Segment 2
    MPLS, Destination address: 172.16.0.1, pw-id: 1, status: Bound
    Pseudowire label: 16001
    Statistics:
      packets: received 0, sent 11799730
      bytes: received 0, sent 707983800
```

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

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


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

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


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


  Nexthop info:
   Base info: version=0xaabbcc14, flags=0x10000, type=5, reserved=0
    nh_addr=172.16.0.1, plat_data_valid=TRUE, plat_data_len=128, child_count=1

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

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

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

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

```
ID   Segment 1         Segment 2
-----------------------------------
1    Gi0/2/0/0 1       10.0.0.1   9)
```

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

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

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

Related Commands

Command	Description
clear l2vpn forwarding counters, on page 66	Clears L2VPN forwarding counters.

show l2vpn forwarding message counters

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

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.

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

Task ID

Task ID	Operation
l2vpn	read

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

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding message counters location 0/1/CPU0
Messages exchanged with L2FIB Collaborators:
-------------------------------------------------------------------------------
     Message                                                Count       Info1         Info2
    Time
     =======                                                =====       =====         =====
    ====
     l2vpn provision messages received:                      0          0x0           0x0
    -
     l2vpn unprovision messages received:                    0          0x0           0x0
    -
     l2vpn bridge provision messages received:               2          0x1           0x0
    Jan  8 14:49:19.283
     l2vpn bridge unprovision messages received:             0          0x0           0x0
    -
     l2vpn bridge main port update messages received:        1          0x2000300     0x0
    Jan  8 12:02:15.628
     l2vpn bridge main port update w/ action=MSTI_DELETE     0          0x0           0x0
```

```
-
 l2vpn bridge main port update ACK sent:             1           0x2000300     0x0
Jan  8 12:02:15.628
 l2vpn bridge port provision messages received:      1           0x2000002     0x0
Jan  8 12:02:15.629
 l2vpn bridge port unprovision messages received:    0           0x0           0x0
-
 l2vpn shg provision messages received:              0           0x0           0x0
-
 l2vpn shg unprovision messages received:            0           0x0           0x0
-
 l2vpn static mac provision messages received:       1           0x0           0x0
Jan  9 08:41:36.668
 l2vpn static mac unprovision messages received:     1           0x0           0x0
Jan  9 08:44:24.208
 l2vpn dynamic mac local learning messages received: 0           0x0           0x0
-
 l2vpn dynamic mac remote learning messages received 0           0x0           0x0
-
 l2vpn dynamic mac refresh messages received:        0           0x0           0x0
-
 l2vpn dynamic mac unprovision messages received:    0           0x0           0x0
-
 AIB update messages received:                       4           0x2000102     0x2000300
Jan  8 12:02:15.622
 AIB delete messages received:                       0           0x0           0x0
-
 FIB nhop registration messages sent:                0           0x0           0x0
-
 FIB nhop unregistration messages sent:              0           0x0           0x0
-
 FIB ecd ldi update messages received:               0           0x0           0x0
-
 FIB invalid NHOP prov messages received:            0           0x0           0x0
-
 Backbone-source-mac prov messages received:         0           0x0           0x0
-
 Backbone-source-mac unprov messages received:       0           0x0           0x0
-
```

Related Commands

Command	Description
clear l2vpn forwarding message counters, on page 68	Clears L2VPN forwarding message counters.

show l2vpn generic-interface-list

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

show l2vpn generic-interface-list {**detail** | **name** | **private** | **summary**}

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
l2vpn	read

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn generic-interface-list
generic-interface-list: l1 (ID: 2, interfaces: 2)  Number of items: 20
generic-interface-list: l2 (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/RSP0/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/RSP0/CPU0:router# show l2vpn generic-interface-list name l1 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 l2vpn index

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

show l2vpn index private

Syntax Description

private	(Optional) Detailed information about all indexes allocated for each pool.

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 index** command:

```
RP/0/RSP0/CPU0:router# show l2vpn 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: 1
```

show l2vpn nsr

To display the status of l2vpn non-stop routing, use the **show l2vpn 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.

Usage Guidelines

To use this command, you must be in a user group associated with a task 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/RSP0/CPU0:router# show l2vpn nsr

Mon May 30 19:32:01.045 UTC
L2VPN NSR information
  NSR Status:
    NSR Ready               : Fri May 27 10:50:59 UTC 2016 (3d08h ago)
    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        : 1
                              PW        : 1
                              BD        : 0
                              MP2MP     : 0
                              RD        : 0
                              PBB       : 0
                              IFLIST    : 0
                              ATOM      : 1
                              Global    : 0
                              PWGroup   : 0
```

```
EVPN        : 0
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
#unique_122	

show l2vpn 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 l2vpn 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
l2vpn	read

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

```
RP/0/RSP0/CPU0:router# show l2vpn 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 Ready               : 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        : 1
                              PW        : 1
                              BD        : 0
                              MP2MP     : 0
                              RD        : 0
                              PBB       : 0
                              IFLIST    : 0
```

```
                              ATOM      : 1
                              Global    : 0
                              PWGroup   : 0
                              EVPN      : 0
  Process Role Change Status:
    Role Change Triggered   : No Role Change
    Role Change Start       : No
    Role Change End         : No
  Process State Transition Time:
    Process-Start           : Mon May 16 10:19:29 PDT 2016 (00:01:02 ago)
    Process-Init            : Mon May 16 10:19:30 PDT 2016 (00:01:01 ago)
    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)
    Run                     : Mon May 16 10:19:58 PDT 2016 (00:00:33 ago)
  Process Collaborator Report Card:
    Collaborator        Connection Status (Since)                              IDT Done
(At)
-------------------------------------------------------------------------------------------

    NSR-INFRA           Up   (Mon May 16 10:19:30 PDT 2016 (00:01:01 ago))      N/A
    NSR-PEER            Down (Never came Up)                                    No
    ISSU-PEER           Down (Never came Up)                                    No
    SYSDB-CONFIG        Up   (Mon May 16 10:19:30 PDT 2016 (00:01:01 ago))      Mon May 16
 10:19:58 PDT 2016 (00:00:33 ago)
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
#unique_122	
show l2vpn index, on page 165	Displays statistics about the index manager.

show l2vpn provision queue

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

show l2vpn 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
l2vpn	read

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

```
RP/0/RSP0/CPU0:router# show l2vpn provision queue

    Legend: P/P/R = Priority/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
VPLS03
```

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

```
RP/0/RSP0/CPU0:router# show l2vpn provision queue standby
    Legend: P/P/R = Priority/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
VPLS03
    BD_NAME                    bd_t                     vpls_bd_class          0/0/0 BD
VPLS04
    BD_NAME                    bd_t                     vpls_bd_class          0/0/0 BD
VPLS05
    BD_NAME                    bd_t                     vpls_bd_class          0/0/0 BD
VPLS06
    BD_NAME                    bd_t                     vpls_bd_class          0/0/0 BD
VPLS07
    BD_NAME                    bd_t                     vpls_bd_class          0/0/0 BD
VPLS08
    BD_NAME                    bd_t                     vpls_bd_class          0/0/0 BD
VPLS09
    BD_NAME                    bd_t                     vpls_bd_class          0/0/0 BD
VPLS010
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.

show l2vpn pw-class

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

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

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

This table describes the significant fields shown in the display.

Table 4: show l2vpn pw-class Command Field Descriptions

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

Field	Description
Protocol	Displays the protocol type.

Related Commands

Command	Description
clear l2vpn forwarding counters, on page 66	Clears L2VPN forwarding counters.

show l2vpn pwhe

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

show l2vpn 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/RSP0/CPU0:router# show l2vpn pwhe detail
Interface: PW-Ether1   Interface State: Down, Admin state: Up
  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
   Gi0/3/0/0, 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/RSP0/CPU0:router# show l2vpn 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 l2vpn resource

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

show l2vpn resource

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

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

Memory: Normal
```

describes the significant fields shown in the display.Table 5: show l2vpn resource Command Field Descriptions, on page 177

Table 5: show l2vpn resource Command Field Descriptions

Field	Description
Memory	Displays memory status.

show l2vpn trace

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

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/RSP0/CPU0:router# show l2vpn 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
node'
    Jul 27 14:39:52.107 l2vpn/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 l2vpn/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 l2vpn/fwd-mac 0/RSP0/CPU0 1# t1  FWD_MAC:1792: Client successfully
 joined gsp group
    Jul 27 14:39:55.340 l2vpn/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 l2vpn/fwd-mac 0/RSP0/CPU0 1# t1  FWD_MAC:626: Entering mac aging
timer init
```

show l2vpn xconnect

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

show l2vpn xconnect [**brief** | **detail** | **encapsulation** | **group** | **groups** | **interface** | **mp2mp** | **mspw** | **neighbor** | **pw-class** | **pw-id** | **state** | **summary** | **type**]

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect
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
Group      Name       ST    Description            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/RSP0/CPU0:router# show l2vpn xconnect detail

Group siva_xc, XC siva_p2p, state is up; Interworking none
  Monitor-Session: pw-span-test, state is configured
  AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none; MSTi 0
    Statistics:
      packet totals: send 90
      byte totals: send 19056
  PW: neighbor 10.1.1.1, PW ID 1, state is up ( established )
    PW class not set, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        30005                          16003
```

```
    Group ID     0x5000300                      0x5000400
    Interface    GigabitEthernet0/4/0/1         GigabitEthernet0/4/0/2
     Interface   pw-span-test                 GigabitEthernet0/3/0/1
    MTU          1500                           1500
    Control word enabled                        enabled
    PW type      Ethernet                       Ethernet
    VCCV CV type 0x2                            0x2
                 (LSP ping verification)        (LSP ping verification)
    VCCV CC type 0x3                            0x3
                  (control word)                 (control word)
                 (router alert label)           (router alert label)
    ------------ ------------------------------ ------------------------------
  Create time: 20/11/2007 21:45:07 (00:49:18 ago)
  Last time status changed: 20/11/2007 21:45:11 (00:49:14 ago)
  Statistics:
    packet totals: receive 0
    byte totals: receive 0

Backup PW:
PW: neighbor 172.16.0.1, PW ID 2, state is up ( established )
  Backup for neighbor 10.0.0.1 PW ID 1 ( standby )
  PW class not set, XC ID 0x0
  Encapsulation MPLS, protocol LDP
  PW type Ethernet, control word enabled, interworking none
  PW backup disable delay 0 sec
  Sequencing not set
      MPLS         Local                          Remote
    ------------ ------------------------------ ------------------------------
    Label        30006                          16003
    Group ID     unassigned                     0x5000400
    Interface    unknown                        GigabitEthernet0/4/0/2
    MTU          1500                           1500
    Control word enabled                        enabled
    PW type      Ethernet                       Ethernet
    VCCV CV type 0x2                            0x2
                 (LSP ping verification)        (LSP ping verification)
    VCCV CC type 0x3                            0x3
                  (control word)                 (control word)
                 (router alert label)           (router alert label)
    ------------ ------------------------------ ------------------------------
  Backup PW for neighbor 10.1.1.1 PW ID 1
  Create time: 20/11/2007 21:45:45 (00:48:40 ago)
  Last time status changed: 20/11/2007 21:45:49 (00:48:36 ago)
  Statistics:
    packet totals: receive 0
    byte totals: receive 0
```

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

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

Group siva_xc, XC siva_p2p, state is down; Interworking none
  Monitor-Session: pw-span-test, state is configured
  AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none; MSTi 0
    Statistics:
      packet totals: send 98
      byte totals: send 20798
  PW: neighbor 10.1.1.1, PW ID 1, state is down ( local ready )
    PW class not set, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
```

```
  PW backup disable delay 0 sec
  Sequencing not set
      MPLS         Local                          Remote
    ------------ ------------------------------ ------------------------------
    Label        30005                          unknown
    Group ID     0x5000300                      0x0
    Interface    GigabitEthernet0/4/0/1         unknown
     Interface     pw-span-test                      GigabitEthernet0/3/0/1
    MTU          1500                           unknown
    Control word enabled                        unknown
    PW type      Ethernet                       unknown
    VCCV CV type 0x2                            0x0
                                                (none)
                 (LSP ping verification)
    VCCV CC type 0x3                            0x0
                                                (none)
                  (control word)
                 (router alert label)
    ------------ ------------------------------ ------------------------------
  Create time: 20/11/2007 21:45:06 (00:53:31 ago)
  Last time status changed: 20/11/2007 22:38:14 (00:00:23 ago)
  Statistics:
    packet totals: receive 0
    byte totals: receive 0

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

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

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

XConnect                        Segment 1                   Segment 2
Group             Name       ST     Description           ST   Description            ST
```

```
------------------------------   --------------------------  -------------------------
g1                x1        UP    pw-span-test          UP   172.16.0.1         1      UP
-----------------------------------------------------------------------------------------
```

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

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

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

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

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

XConnect                   Segment 1                   Segment 2
Group      Name       ST   Description            ST   Description            ST
------------------------   --------------------------   ------------------------
siva_xc    siva_p2p   UP   Gi0/4/0/1              UP   10.0.0.1         1     UP
                                                       Backup
                                                       172.16.0.1       2     UP
-----------------------------------------------------------------------------
```

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

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

Group siva_xc, XC siva_p2p, state is up; Interworking none
  AC: GigabitEthernet0/4/0/1, state is up
```

```
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none; MSTi 0
    Statistics:
      packet totals: received 90, sent 90
      byte totals: received 19056, sent 19056
  PW: neighbor 10.0.0.1, PW ID 1, state is up ( established )
    PW class not set, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        30005                          16003
      Group ID     0x5000300                      0x5000400
      Interface    GigabitEthernet0/4/0/1         GigabitEthernet0/4/0/2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ ------------------------------
    Create time: 20/11/2007 21:45:07 (00:49:18 ago)
    Last time status changed: 20/11/2007 21:45:11 (00:49:14 ago)
    Statistics:
      packet totals: received 0, sent 0
      byte totals: received 0, sent 0

  Backup PW:
  PW: neighbor 172.16.0.1, PW ID 2, state is up ( established )
    Backup for neighbor 10.0.0.1 PW ID 1 ( standby )
    PW class not set, XC ID 0x0
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        30006                          16003
      Group ID     unassigned                     0x5000400
      Interface    unknown                        GigabitEthernet0/4/0/2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ ------------------------------
    Backup PW for neighbor 10.0.0.1 PW ID 1
    Create time: 20/11/2007 21:45:45 (00:48:40 ago)
    Last time status changed: 20/11/2007 21:45:49 (00:48:36 ago)
    Statistics:
      packet totals: received 0, sent 0
      byte totals: received 0, sent 0
```

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

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

```
Group siva_xc, XC siva_p2p, state is down; Interworking none
  AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none; MSTi 0
    Statistics:
      packet totals: send 98
      byte totals: send 20798
  PW: neighbor 10.0.0.1, PW ID 1, state is down ( local ready )
    PW class not set, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        30005                          unknown
      Group ID     0x5000300                      0x0
      Interface    GigabitEthernet0/4/0/1         unknown
      MTU          1500                           unknown
      Control word enabled                        unknown
      PW type      Ethernet                       unknown
      VCCV CV type 0x2                            0x0
                                                  (none)
                   (LSP ping verification)
      VCCV CC type 0x3                            0x0
                                                  (none)
                    (control word)
                   (router alert label)
      ------------ ------------------------------ ------------------------------
    Create time: 20/11/2007 21:45:06 (00:53:31 ago)
    Last time status changed: 20/11/2007 22:38:14 (00:00:23 ago)
    Statistics:
      packet totals: received 0, sent 0
      byte totals: received 0, sent 0

  Backup PW:
  PW: neighbor 172.16.0.1, PW ID 2, state is up ( established )
    Backup for neighbor 10.0.0.1 PW ID 1 ( active )
    PW class not set, XC ID 0x0
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        30006                          16003
      Group ID     unassigned                     0x5000400
      Interface    unknown                        GigabitEthernet0/4/0/2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x3                            0x3
                    (control word)                 (control word)
                   (router alert label)           (router alert label)
      ------------ ------------------------------ ------------------------------
    Backup PW for neighbor 10.0.0.1 PW ID 1
    Create time: 20/11/2007 21:45:44 (00:52:54 ago)
    Last time status changed: 20/11/2007 21:45:48 (00:52:49 ago)
    Statistics:
      packet totals: received 0, sent 0
```

```
      byte totals: received 0, sent 0
```

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

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

Group VPWS, XC ac3, state is up; Interworking none
AC: GigabitEthernet0/7/0/5.3, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [12, 12]
MTU 1508; XC ID 0x2440096; interworking none
Statistics:
packets: received 26392092, sent 1336
bytes: received 1583525520, sent 297928
drops: illegal VLAN 0, illegal length 0
PW: neighbor 192.168.0.1, PW ID 3, state is up ( established )
PW class VPWS1, XC ID 0x2440096
Encapsulation MPLS, protocol LDP
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

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

This table describes the significant fields shown in the display.

Table 6: show l2vpn xconnect Command Field Descriptions

Field	Description
XConnect Group	Displays a list of all configured cross-connect groups.
Group	Displays the cross-connect group number.

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

Related Commands

Command	Description
xconnect group, on page 206	Configures cross-connect groups.

show tech-support l2vpn platform no-statistics

To automatically run show commands that display information specific to Layer 2 Virtual Private Network (L2VPN) platform without debugging statistics, use the **show tech-support l2vpn platform no-statistics** command in the EXEC mode.

show tech-support l2vpn platform no-statistics [**file** | **list-CLIs** | **location** | **rack**]

Syntax Description

file	Specifies that the command output is saved to a specified file.
list-CLIs	Specifies the list of CLIs but not executed.
location	Specifies a location.
rack	Specifies a rack.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

This command collects information for Layer 2 VPN platform related issues that is useful for Cisco Technical Support representatives when troubleshooting a router.

Note The **show tech-support l2vpn platform** command does not collect all bridge domains information when there is large scale values associated with bridge domains. Hence, use the **show tech-support l2vpn platform no-statistics** command.

Task ID

Task ID	Operation
l2vpn	read

Example

The following example shows the output of **show tech-support l2vpn platfrom no-statistics** command.

```
RP/0/RSP0/CPU0:router#show tech-support l2vpn platfrom no-statistics

Tue Jan  8 02:40:56.007 UTC
++ Show tech start time: 2019-Jan-08.024056.UTC ++
Tue Jan 08 02:40:56 UTC 2019 Waiting for gathering to complete
```

```
.............................
Tue Jan 08 02:43:03 UTC 2019 Compressing show tech output
Show tech output available at 0/RSP1/CPU0 :
/net/node0_RSP1_CPU0/harddisk:/showtech/showtech-RR-l2vpn_platform-2019-Jan-08.024056.UTC.tgz
++ Show tech end time: 2019-Jan-08.024303.UTC ++
```

source (p2p)

To configure source IPv6 address of the pseudowire, use the **source** command in p2p pseudowire configuration mode. To disable the source IPv6 address configuration, use the **no** form of this command.

source *ipv6_address*
no source *ipv6_address*

Syntax Description

ipv6_address	Source IPv6 address of pseudowire

Command Default

None

Command Modes

p2p pseudowire 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	Operation
l2vpn	read, write

Example

This example shows how to set a source IPv6 address to a point-to-point IPv6 cross-connect:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group g1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p xc3
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/4.2
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# source 1111:2222::abcd
```

Related Commands

Command	Description
p2p, on page 122	Enters p2p configuration submode to configure point-to-point cross-connects.
neighbor (L2VPN), on page 103	Configures a pseudowire for a cross-connect.

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

l2vpn 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
l2vpn	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)# l2vpn
RP/0/RSP0/CPU0:a9k1(config-l2vpn)# bridge group BG1
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg)# bridge-domain BD1
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd)# storm-control unknown-unicast pps 100
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd)# storm-control multicast pps 100
RP/0/RSP0/CPU0:a9k1(config-l2vpn-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)# l2vpn
RP/0/RSP0/CPU0:a9k1(config-l2vpn)# bridge group BG1
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd)# bridge-domain BD2
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd)# interface Bundle-Ether9001.2001
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd-ac)# storm-control unknown-unicast pps 100
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd-ac)# storm-control multicast pps 100
RP/0/RSP0/CPU0:a9k1(config-l2vpn-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)# l2vpn
RP/0/RSP0/CPU0:a9k1(config-l2vpn)# bridge group BG1
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd)# bridge-domain BD2
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd-ac)# neighbor 10.1.1.1 pw-id 20011001
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd-pw)# storm-control unknown-unicast pps 100
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd-pw)# storm-control multicast pps 100
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd-pw)# storm-control broadcast pps 100
RP/0/RSP0/CPU0:a9k1(config-l2vpn-bg-bd-pw)# commit
```

Running Configuration

```
l2vpn
 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)#
```

switching-tlv (L2VPN)

To advertise the switching point type-length variable (TLV) in the label binding, use the **switching-tlv** command in the pseudowire class configuration mode. To disable the display of the TLV, use the **no** form of this command.

switching tlv hide
no switching tlv

Syntax Description

hide	Hides TLV.

Command Default

Switching point TLV data is advertised to peers.

Command Modes

L2VPN pseudowire class encapsulation mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The pseudowire switching point TLV information includes the following information:

- Pseudowire ID of the last pseudowire segment traversed
- Pseudowire switching point description
- Local IP address of the pseudowire switching point
- Remote IP address of the last pseudowire switching point that was crossed or the T-PE router

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)# switching-tlv hide
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)#
```

Related Commands

Command	Description
pw-class (L2VPN), on page 113	Enters pseudowire class submode to define a pseudowire class template.

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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group xc1
RP/0/RSP0/CPU0:router(config-l2vpn-xc)#p2p grp1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)#neighbor 10.1.1.2 pw-id 78
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)#tag-impose vlan 8
```

Related Commands

Command	Description
pw-class (L2VPN), on page 113	Enters pseudowire class submode to define a pseudowire class template.

tos (l2vpn)

To configure Type of Service (TOS) reflection or to set TOS value, use the **tos** command in L2VPN pseudowire class encapsulation L2TPv3 configuration mode. To reset the TOS value, use the **no** form of this command.

tos {**reflect** [**value** *tos value*] | **value** *tos value* [**reflect**]}
no tos {**reflect** [**value** *tos value*] | **value** *tos value* [**reflect**]}

Syntax Description

reflect	Enables TOS reflection.
value	Sets the TOS value for L2TPv3 pseudowire class.
tos value	Value of the TOS.

Command Default

By default, the TOS is copied over, from the class of service (COS) fields of the VLAN header. If the underlying packet is not an IPv4 or IPv6 packet, the COS fields are copied from the VLAN header, even if TOS reflection is configured.

Command Modes

L2VPN pseudowire class encapsulation L2TPv3 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	Operation
l2vpn	read, write

Example

This example shows how to configure TOS reflection:

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-l2tpv3)# protocol l2tpv3
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-l2tpv3)# tos reflect
```

The following example shows how to set a TOS value:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation l2tpv3
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-l2tpv3)# protocol l2tpv3
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-l2tpv3)# tos value 64
```

transport mode (L2VPN)

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN pseudowire class MPLS encapsulation

Command History

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

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to configure Ethernet transport mode:

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

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

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

Related Commands

Command	Description
pw-class (L2VPN), on page 113	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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group bg1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bd1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# transport mode vlan passthrough
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

ttl (l2vpn)

To configure Time to Live (TTL) for Pseudowire class, use the **ttl** command in L2VPN pseudowire class encapsulation L2TPv3 configuration mode. To disable the TTL configuration, use the **no** form of this command.

ttl *ttl _value*
no ttl *ttl_value*

Syntax Description

ttl_value	The TTL Value. Range is from 1 to 255.

Command Default

None

Command Modes

L2VPN pseudowire class encapsulation L2TPv3 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	Operation
l2vpn	read, write

Example

This example shows how to configure TTL:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class kanata01
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation l2tpv3
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-l2tpv3)# protocol l2tpv3
RP/0/RSP0/CPU0:router(config-l2vpn-pwc-l2tpv3)# ttl 40
```

vpws-seamless-integration

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

vpws-seamless-integration

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
L2VPN	read, write

Examples

The following example shows how to enable EVPN-VPWS integration on an edge device for BGP PW.

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

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

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

xconnect group

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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



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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
show l2vpn xconnect, on page 180	Displays brief information on configured cross-connects.



Multipoint Layer 2 Services Commands

- action (VPLS), on page 209
- aging (VPLS), on page 211
- aps-channel, on page 213
- autodiscovery bgp, on page 215
- bridge-domain (VPLS), on page 216
- bridge group (VPLS), on page 217
- clear l2vpn bridge-domain (VPLS), on page 218
- coupled-mode, on page 219
- debug l2vpn forwarding platform vpls all location, on page 221
- description (G.8032), on page 222
- dhcp ipv4 snoop profile (VPLS), on page 223
- ethernet ring g8032, on page 225
- ethernet ring g8032 profile, on page 226
- exclusion list, on page 228
- flooding disable, on page 229
- flooding unknown-unicast disable (VPLS), on page 231
- igmp snooping disable, on page 233
- inclusion-list, on page 234
- instance (G.8032), on page 236
- interface (VPLS), on page 237
- l2vpn resynchronize forwarding mac-address-table location, on page 239
- learning disable (VPLS), on page 240
- level, on page 242
- limit (VPLS), on page 243
- mac (VPLS), on page 245
- mac secure, on page 247
- maximum (VPLS), on page 250
- monitor interface (port0), on page 252
- monitor interface (port1), on page 253
- mpls static label (VPLS), on page 254
- mtu (VPLS), on page 256
- multicast p2mp, on page 258
- neighbor (VPLS), on page 260

- notification (VPLS), on page 262
- open ring, on page 264
- port0 interface, on page 265
- port1, on page 266
- port-down flush disable (VPLS), on page 267
- profile, on page 269
- pw-class , on page 270
- pw-oam, on page 272
- pw-status (L2VPN), on page 273
- route-target, on page 275
- routed, on page 277
- rpl, on page 278
- show ethernet ring g8032, on page 280
- show l2vpn bridge-domain (VPLS), on page 283
- show l2vpn ethernet ring g8032, on page 294
- show l2vpn forwarding bridge-domain (VPLS), on page 296
- show l2vpn forwarding bridge-domain mac-address (VPLS), on page 299
- show l2vpn forwarding ethernet ring g8032, on page 303
- show l2vpn forwarding protection main-interface, on page 305
- show l2vpn protection main-interface, on page 307
- shutdown (Bridge Domain), on page 310
- shutdown (VFI), on page 311
- signaling-protocol, on page 313
- split-horizon group, on page 315
- static-address (VPLS), on page 317
- static-mac-address (VPLS), on page 319
- tcn-propagation, on page 321
- time (VPLS), on page 322
- transport rsvp-te, on page 324
- type (VPLS), on page 326
- vfi (VPLS), on page 328
- withdraw (VPLS), on page 330

action (VPLS)

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

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

Syntax Description

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

Command Default

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

Command Modes

L2VPN bridge group bridge domain MAC limit configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	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 243	Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 250	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 262	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 322 and the type (VPLS), on page 326 parameters.

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Commands	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.

Commands	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then assigns network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.
time (VPLS), on page 322	Configures the maximum aging time.
type (VPLS), on page 326	Configures the type for MAC address aging.

aps-channel

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

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

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

Related Commands

Command	Description
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.
inclusion-list, on page 234	Associates a set of VLAN IDs with the current instance.

autodiscovery bgp

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

autodiscovery bgp
no autodiscovery bgp

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

VFI configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure a bridge domain:

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

bridge-domain (VPLS)

To establish a bridge domain and to enter L2VPN bridge group bridge domain configuration mode, use the **bridge-domain** command in L2VPN bridge group configuration mode. To return to a single bridge domain, use the **no** form of this command.

bridge-domain *bridge-domain-name*
no bridge-domain *bridge-domain-name*

Syntax Description

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

Command Default

The default value is a single bridge domain.

Command Modes

L2VPN bridge group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure a bridge domain:

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

Related Commands

Command	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

bridge group (VPLS)

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

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

Syntax Description

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

Command Default

No bridge group is created.

Command Modes

L2VPN configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows that bridge group 1 is assigned:

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
l2vpn, on page 92	Enters L2VPN configuration mode.

clear l2vpn bridge-domain (VPLS)

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
show l2vpn bridge-domain (VPLS), on page 283	Display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains.

coupled-mode

To enable coupled mode, use the **coupled-mode** command in the L2VPN bridge group bridge domain configuration mode.

coupled-mode

Syntax Description

This command has no keywords or arguments.

Command Default

Coupled mode is disabled. VPLS bridge domains use decoupled behavior by default.

Command Modes

L2VPN bridge group bridge domain configuration mode

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

Use this command when the VPLS Virtual Forwarding Instance (VFI) and its core pseudowires (PWs) must follow the availability of the eligible local attachment set in the bridge-domain.

- When coupled mode is configured and at least one eligible local attachment circuit (AC) or access PW is up, the bridge-domain coupled state is up, and the VFI and core PWs stay up.
- When coupled mode is configured and no eligible local AC or access PW is present or up, the bridge-domain coupled state is down, and the VFI and core PWs go down.
- When coupled mode is not configured, the bridge-domain coupled state is disabled, and VPLS uses decoupled behavior.
- Use the **show l2vpn bridge-domain** command with the **detail** keyword to verify the coupled state.

Task ID	Operation
l2vpn	read, write

Enable coupled mode

This example enables coupled mode for a VPLS bridge domain with one local attachment and one VFI neighbor.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group BG_VPLS
Router(config-l2vpn-bg)# bridge-domain BD_VPLS
Router(config-l2vpn-bg-bd)# coupled-mode
Router(config-l2vpn-bg-bd)# interface TenGigE0/0/0/32.100
Router(config-l2vpn-bg-bd)# vfi VFI_VPLS
Router(config-l2vpn-bg-bd-vfi)# neighbor 192.0.2.6 pw-id 20100
Router(config-l2vpn-bg-bd-vfi-pw)# commit
```

Disable coupled mode

This example restores the default decoupled behavior for a VPLS bridge domain.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group BG_VPLS
Router(config-l2vpn-bg)# bridge-domain BD_VPLS
Router(config-l2vpn-bg-bd)# no coupled-mode
Router(config-l2vpn-bg-bd)# commit
```

Verify the coupled state

This example displays the coupled state for a VPLS bridge domain.

```
Router# show l2vpn bridge-domain bd-name BD_VPLS detail
Legend: pp = Partially Programmed.
Bridge group: BG_VPLS, bridge-domain: BD_VPLS, id: 4, state: up, ShgId: 0, MSTi: 0
  Coupled state: up
```

debug l2vpn forwarding platform vpls all location

To display debugging information about L2VPN forwarding Virtual Private LAN Service (VPLS) platform of a specified location, use the **debug l2vpn forwarding platform vpls all location** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug l2vpn forwarding platform vpls all location *location*
no debug l2vpn forwarding platform vpls all location *location*

Syntax Description

location	Location to dispaly debugging information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.1	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
root-system	read, write

description (G.8032)

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

description *ring-instance-identifier*

Syntax Description

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

Command Default

None

Command Modes

Ethernet ring G.8032 instance configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.
instance (G.8032), on page 236	Configures a G.8032 Ethernet ring instance and enters Ethernet ring G.8032 instance configuration submode.

dhcp ipv4 snoop profile (VPLS)

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

dhcp ipv4 snoop profile *profile-name*
no dhcp ipv4 snoop

Syntax Description

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

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#vfi vf1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)#exit
```

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

ethernet ring g8032

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

ethernet ring g8032 *protocol ring identifier*
no ethernet ring g8032 *protocol ring identifier*

Syntax Description

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

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Example

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

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

Related Commands

Command	Description
exclusion list, on page 228	Defines a set of Virtual LAN (VLAN) IDs that are not protected by the Ethernet ring protection mechanism.
instance (G.8032), on page 236	Configures a G.8032 Ethernet ring instance and enters Ethernet ring G.8032 instance configuration submode.
port0 interface, on page 265	Enables G.8032 for a specified ring port.
port1, on page 266	Enables G.8032 for a specified ring port.

ethernet ring g8032 profile

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

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

Syntax Description

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

Command Default

None

Command Modes

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ethernet-services	read, write

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

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

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

Related Commands

Command	Description
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

exclusion list

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

exclusion list vlan-ids *vlan range*
no exclusion list vlan-ids *vlan range*

Syntax Description

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

Command Default

Configured physical Ethernet or ether bundle interface

Command Modes

Ethernet ring g8032 configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows the output from the exclusion list command:

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

Related Commands

Command	Description
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

flooding disable

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

flooding disable
no flooding disable

This command has no keywords or arguments.

Command Default

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

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mtu (VPLS), on page 256	Adjusts the maximum packet size or maximum transmission unit (MTU) size for the bridge domain.

flooding unknown-unicast disable (VPLS)

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

flooding unknown-unicast disable
no flooding unknown-unicast disable

Syntax Description

This command has no keywords or arguments.

Command Default

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

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

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

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mtu (VPLS), on page 256	Adjusts the maximum packet size or maximum transmission unit (MTU) size for the bridge domain.

igmp snooping disable

To disable IGMP snooping on a bridge domain within the L2VPN, use the **igmp snooping disable** command in the L2VPN bridge group bridge-domain configuration mode. To return to the default, use the **no** form of this command.

igmp snooping disable
no igmp snooping disable

Syntax Description

This command has no keywords or arguments.

Command Default

IGMP snooping is active on a bridge domain when an IGMP snooping profile is configured to the bridge domain.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 5.1	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 disable IGMP snooping profile for a bridge domain in the L2VPN:

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

inclusion-list

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

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

Syntax Description

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

Command Default

None

Command Modes

Ethernet ring G.8032 instance configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

Command	Description
instance (G.8032), on page 236	Configures a G.8032 Ethernet ring instance and enters Ethernet ring G.8032 instance configuration submode.

instance (G.8032)

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

instance *instance-id*
no instance *instance-id*

Syntax Description

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

Command Default

None

Command Modes

Ethernet ring G.8032 configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

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

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

Related Commands

Command	Description
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.
l2vpn, on page 92	Enters L2VPN configuration mode.

interface (VPLS)

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

l2vpn resynchronize forwarding mac-address-table location

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
l2vpn	read, write, execute

Examples

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

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

Related Commands

Command	Description
show l2vpn forwarding, on page 154	Displays forwarding information from the layer2_fib manager on the line card.

learning disable (VPLS)

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

learning disable
no learning disable

Syntax Description

This command has no keywords or arguments.

Command Default

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

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.

level

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

level *number*

Syntax Description

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

Command Default

None

Command Modes

Ethernet ring G.8032 instance aps-channel configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

limit (VPLS)

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

limit
no limit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# limit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# maximum 100
```

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

Related Commands

Command	Description
action (VPLS), on page 209	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 250	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 262	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

mac (VPLS)

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

mac
no mac

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
aging (VPLS), on page 211	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
learning disable (VPLS), on page 240	Overrides the MAC learning configuration of a parent bridge or sets the MAC learning configuration of a bridge.
limit (VPLS), on page 243	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 317	Adds static entries to the MAC address for filtering.
withdraw (VPLS), on page 330	Disables MAC address withdrawal for a specified bridge domain

mac secure

To configure MAC security at a port and to set the default action that is to be taken when security is violated, use the **mac secure** command in the L2VPN bridge group bridge domain configuration mode. Starting from Cisco IOS XR Release 7.5.2, you can use the command in the EVPN configuration mode as well.

To disable MAC security, use the **no** form of this command.

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

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

Syntax Description

action	(Optional) Indicates the action to be taken when security is violated.
none	Forwards the violating packet and allows the MAC address to be relearned.
shutdown	Shuts down the violating bridge port.
restrict	Drops the violating packet and disables the learn attempt. **Note** The **restrict** keyword in applicable to interfaces only.
logging	(Optional) Enables logging.
disable	(Optional) Disables mac security.
shutdown-recovery-timeout *timer-value*	Sets the Recovery timer to revert shutdown action automatically after the timer expires. Recovery timer value can be set in the range of 10 to 3600 seconds.

To configure MAC security in the EVPN configuration mode use:

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

Syntax Description

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

disable	Disable duplicate detection of MAC address.

Command Default

When configured in the L2VPN bridge-group, bridge-domain configuration moe, if a MAC address has been learned on a secure port and, a relearn attempt from another port (secure or not) is made, the default action is **restrict**.

Command Modes

L2VPN bridge group bridge domain configuration

EVPN configuration

Command History

Release	Modification
Release 4.0.1	This command was introduced.
Release 6.6.1	The keyword **shutdown-recovery-timeout** *timer-value* was introduced.
Release 7.5.2	The command was modifed to support EVPN configuration mode.

Usage Guidelines

The MAC security recovery applies only for the Ethernet flow point (EFP) security. The Shutdown recovery timer does not apply to MAC limits configured on a per-EFP level, per-bridge domain level, or both.

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

Task ID

Task ID	Operations
l2vpn	Read, write

Examples

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

```
Router# configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group b1
Router(config-l2vpn-bg)#bridge-domain bar
Router(config-l2vpn-bg-bd)#mac secure
Router(config-l2vpn-bg-bd-mac-secure)#
```

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

```
Router#configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group b1
Router(config-l2vpn-bg)#bridge-domain bar
Router(config-l2vpn-bg-bd)#mac secure
Router(config-l2vpn-bg-bd-mac-secure)#action shutdown
Router(config-l2vpn-bg-bd-mac-secure)#
```

This example shows how to bring up or recover the bridge port that was shut down due to security violation.

```
Router(config-l2vpn-bg-bd-mac-secure)# interface GigabitEthernet0/0/0/5.11
Router(config-l2vpn-bg-bd-ac)# mac
Router(config-l2vpn-bg-bd-ac-mac)# secure
Router(config-l2vpn-bg-bd-ac-mac-secure)# action shutdown
Router(config-l2vpn-bg-bd-ac-mac-secure)# logging
Router(config-l2vpn-bg-bd-ac-mac-secure)# shutdown-recovery-timeout 600
Router(config-l2vpn-bg-bd-ac-mac-secure)#     !
```

Examples

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

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

maximum (VPLS)

To configure the specified action when the number of MAC addresses learned on a bridge is reached, use the **maximum** command in L2VPN bridge group bridge domain MAC limit configuration mode. To disable this feature, use the **no** form of this command.

maximum *value*
no maximum *value*

Syntax Description

value	Maximum number of learned MAC addresses. The range is from 5 to 512000.

Command Default

The default maximum value is 4000.

Command Modes

L2VPN bridge group bridge domain MAC limit configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

The action can either be flood, no flood, or shutdown. Depending on the configuration, a syslog, an SNMP trap notification, or both are issued.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows when the number of MAC address learned on the bridge reaches 5000 and the bridge stops learning but continues flooding:

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# maximum 5000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# action no-flood
```

Related Commands

Command	Description
action (VPLS), on page 209	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
limit (VPLS), on page 243	Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.
notification (VPLS), on page 262	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

monitor interface (port0)

To specify a port to detect a ring link failure, use the **monitor interface** command in g8032 port0 submode. To delete the port, use the **no** form of this command.

monitor interface *interface-name*
no monitor interface *interface-name*

Syntax Description

interface-name	Name of the monitored interface. The monitored interface must be a sub-interface of the main interface.

Command Default

Configured physical Ethernet or Ether Bundle interface

Command Modes

Ethernet ring g8032 port0 submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows the output from the monitor interface command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# port0 interface TenGigE 0/4/0/0
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port0)# monitor interface GigabitEthernet 0/0/1/0
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port0)#
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

monitor interface (port1)

To specify the port to detect a ring link failure, use the **monitor interface** command in g8032 port1 submode. To delete the port, use the **no** form of this command.

monitor interface *interface-name*
no monitor interface *interface-name*

Syntax Description

interface-name	Name of the monitored interface. The monitored interface must be a sub-interface of the main interface.

Command Default

Configured physical Ethernet or ether bundle interface

Command Modes

Ethernet ring g8032 port1 submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows the output from the monitor interface command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# port1 interface TenGigE 0/4/0/0
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port1)# monitor interface GigabitEthernet 0/0/1/0
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port1)#
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

mpls static label (VPLS)

To configure the MPLS static labels and the static labels for the access pseudowire configuration, use the **mpls static label** command in L2VPN bridge group bridge domain VFI pseudowire configuration mode. To assign the dynamic MPLS labels to either the virtual forwarding interface (VFI) pseudowire or the access pseudowire, use the **no** form of this command.

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

Syntax Description

local *value*	Configures the local pseudowire label. **Note** Use the **show mpls label range** command to obtain the range for the local labels.
remote *value*	Configures the remote pseudowire label. **Note** The range of values for the remote labels depends on the label allocator of the remote router.

Command Default

By default, the router attempts to assign dynamic labels to the pseudowire.

Command Modes

L2VPN bridge group bridge domain Access/VFI pseudowire configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the VFI pseudowire 10.1.1.2 with pseudowire ID of 1000 to use MPLS label 800 and remote MPLS label 500:

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi model
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# mpls static label local 800 remote 500
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
neighbor (VPLS), on page 260	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
pw-class , on page 270	Configures the pseudowire class template name to use for the pseudowire.
vfi (VPLS), on page 328	Configures virtual forwarding interface (VFI) parameters.

mtu (VPLS)

To adjust the maximum packet size or maximum transmission unit (MTU) size for the bridge domain, use the **mtu** command in L2VPN bridge group bridge domain configuration mode. To disable this feature, use the **no** form of this command.

mtu *bytes*
no mtu

Syntax Description

bytes	MTU size, in bytes. The range is from 46 to 65535.

Command Default

The default MTU value is 1500.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies, but cannot be set smaller than 64 bytes.

The MTU for the bridge domain includes only the payload of the packet. For example, a configured bridge MTU of 1500 allows tagged packets of 1518 bytes (6 bytes DA, 6 bytes SA, 2 bytes ethertype, or 4 bytes qtag).

Note Bridge wide MTU is not enforced on the data traffic.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example specifies an MTU of 1000 bytes:

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mtu 1000
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	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 229	Configures flooding for traffic at the bridge domain level or at the bridge port level.
l2vpn, on page 92	Enters L2VPN configuration mode.

multicast p2mp

To enable point to multi-point pseudowire in a VFI and to enter L2VPN bridge group bridge domain VFI multicast P2MP configuration mode, use the **multicast p2mp** command in L2VPN bridge group bridge domain VFI configuration mode. To return to a VFI mode, use the **no** form of this command.

multicast p2mp [**signaling-protocol** | **transport**]
no multicast p2mp [**signaling-protocol** | **transport**]

Syntax Description

signaling-protocol	Specifies the signaling protocol selection
transport	Specifies the transport type selection

Command Default

None

Command Modes

L2VPN bridge group bridge domain VFI configuration

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to configure a point to multi-point pseudowire in a VFI:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# multicast p2mp
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-p2mp)#
```

Related Commands

Command	Description
transport rsvp-te, on page 324	Enables RSVP-TE as transport on a VFI.

Command	Description
vfi (VPLS), on page 328	Configures virtual forwarding interface (VFI) parameters.
bridge-domain (VPLS), on page 216	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

neighbor (VPLS)

To add an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI), use the **neighbor** command in the appropriate L2VPN bridge group bridge domain configuration submode. To remove the pseudowire either from the bridge or from the VFI, use the **no** form of this command.

neighbor *A.B.C.D* **pw-id** *value*
no neighbor *A.B.C.D* **pw-id** *value*

Syntax Description

A.B.C.D	IP address of the cross-connect peer.
pw-id *value*	Configures the pseudowire ID and ID value. Range is 1 to 4294967295.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

L2VPN bridge group bridge domain VFI configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Use the **neighbor** command to enter L2VPN bridge group bridge domain VFI pseudowire configuration mode. Alternatively, use the **neighbor** command to enter L2VPN bridge group bridge domain access pseudowire configuration mode.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure an access pseudowire directly under a bridge domain in L2VPN bridge group bridge domain configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)#
```

The following example shows how to configure the parameters for any pseudowire in L2VPN bridge group bridge domain VFI configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 254	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
pw-class , on page 270	Configures the pseudowire class template name to use for the pseudowire.
static-mac-address (VPLS), on page 319	Configures the static MAC address to associate a remote MAC address with a pseudowire or any other bridge interface.
vfi (VPLS), on page 328	Configures virtual forwarding interface (VFI) parameters.

notification (VPLS)

To specify the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit, use the **notification** command in L2VPN bridge group bridge domain MAC limit configuration mode. To use the notification as only a syslog entry, use the **no** form of this command.

notification {**both** | **none** | **trap**}
no notification {**both** | **none** | **trap**}

Syntax Description

both	Sends syslog and trap notifications when the action is violated.
none	Specifies no notification.
trap	Sends trap notifications when the action is violated.

Command Default

By default, only a syslog message is sent when the number of learned MAC addresses reaches the maximum configured.

Command Modes

L2VPN bridge group bridge domain MAC limit configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

A syslog message and an SNMP trap is generated. Alternatively, an SNMP trap is generated. Finally, no notification is generated.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how both a syslog message and an SNMP trap are generated with the bridge bar and learns more MAC addresses than the configured limit:

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

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

Related Commands

Command	Description
action (VPLS), on page 209	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 250	Configures the specified action when the number of MAC addresses learned on a bridge is reached.

open ring

To specify Ethernet ring g8032 as an open ring, use the **open-ring** command in Ethernet ring g8032 configuration submode. To delete, use the **no** form of this command.

open-ring
no open-ring

This command has no keywords or arguments.

Command Default

The default value is FALSE.

Command Modes

Ethernet ring g8032 configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows the output from the **open-ring** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# open-ring
RP/0/RSP0/CPU0:router(config-l2vpn-erp)#
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

port0 interface

To enable G.8032 for a specified ring port, use the **port0 interface** command in g8032 configuration port0 submode. To disable, use the **no** form of this command.

port 0 interface *interface name*
no port 0 interface *interface name*

Syntax Description

interface name	Any physical Ethernet or Bundle Ethernet interface. A physical port of the local node connected to G.8032 ring.

Command Default

None

Command Modes

Ethernet ring g8032 configuration port0 submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows the output from the port0 interface command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# port0 interface Bundle-Ether 555
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port0)#
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

port1

To enable G.8032 for a specified ring port, use the **port1** command in g8032 configuration port1 submode. To disable, use the **no** form of this command.

port1 {**interface** *interface name* | **none**}

Syntax Description

interface *interface name*	Specifies physical Ethernet or Bundle Ethernet interface. A physical port of the local node connected to G.8032 ring. Enables G.8032 for the specified physical port to form a closed ring.
none	Specifies local node endpoint of an open-ring.

Command Default

None

Command Modes

Ethernet ring g8032 configuration port1 submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows the output from the port1 command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-l2vpn-erp)# port1 interface TenGigE 0/6/0/3
RP/0/RSP0/CPU0:router(config-l2vpn-erp-port1)#
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

port-down flush disable (VPLS)

To disable MAC flush when the bridge port is nonfunctional, use the **port-down flush disable** command in the L2VPN bridge group bridge domain MAC configuration mode. Use the **no** form of this command to enable the MAC flush when the bridge port is nonfunctional.

port-down flush disable
no port-down flush disable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

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

The **port-down flush disable** command disables the MAC flush when the bridge port is nonfunctional.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

Related Commands

Command	Description
action (VPLS), on page 209	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 250	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 262	Specifies the type of notification that is sent when the number of learned MAC addresses exceeds the configured limit.

profile

To specify an associated Ethernet ring G.8032 profile, use the **profile** command in the Ethernet ring G.8032 instance configuration submode.

profile *profile-name*

Syntax Description

profile-name	Ethernet ring G.8032 profile name.

Command Default

None

Command Modes

Ethernet ring G.8032 instance configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to specify a G.8032 ring profile name:

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

pw-class

To configure the pseudowire class template name to use for the pseudowire, use the **pw-class** command in L2VPN bridge group bridge domain Access pseudowire configuration mode. To delete the pseudowire class, use the **no** form of this command.

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

Syntax Description

class-name	Pseudowire class name.

Command Default

None

Command Modes

L2VPN bridge group bridge domain Access pseudowire configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# pw-class canada
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 254	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 260	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
vfi (VPLS), on page 328	Configures virtual forwarding interface (VFI) parameters.

pw-oam

To enable the Operations, Administration, and Maintenance (OAM) feature on a pseudowire for defect notifications, use the **pw-oam** command in L2VPN configuration submode. To disable the feature, use the **no** form of this command.

pw-oam refresh transmit *value*
no pw-oam refresh transmit *value*

Syntax Description

refresh transmit	Refresh interval when outbound pseudowire status messages are transmitted.
value	Interval value in seconds. The range is from 1 to 4095. The default value is 30.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enable the oam feature on a pseudowire:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-oam refresh transmit
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-oam refresh transmit 456
```

Related Commands

Command	Description
pw-class (L2VPN), on page 113	Enters pseudowire class submode to define a pseudowire class template.

pw-status (L2VPN)

To enable status signaling on a pseudowire, use the **pw-status** command in L2VPN configuration submode. To disable the pseudowire status signaling, use the **no** form of this command.

pw-status
no pw-status

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Cisco IOS XR software provides two methods for signaling pseudowires (PW) status:

- Using Label Withdraw Message

  The provider edge routers (PEs) send Label Mapping Message to their peers as soon as the pseudowire is configured and administratively enabled. The pseudowire label should not be withdrawn unless the pseudowire is administratively disabled or deleted.

- Using PW status TLV

  The PEs use LDP pseudowire status TLV to indicate pseudowire status to their peers. The LDP pseudowire status TLV contains additional information compared to the Label Withdraw Message.



Note Unless pseudowire status TLV is explicitly enabled under L2VPN configuration, the default signaling method is Label Withdrawal.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable pseudowire status signaling on configured pseudowires:

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.

route-target

To specify a route target for the VFI, use the **route-target** command in the BGP autodiscovery mode. To return to the default value, use the **no** form of this command.

route-target {*as-number:nn* *ip-address:nn* }
no route-target {*as-number:nn* *ip-address:nn* }

Syntax Description

as-number:nn Autonomous system (AS) number of the route distinguisher.

- as-number—16-bit AS number

  Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535.

- nn—32-bit number

ip-address:nn IP address of the route distinguisher.

- ip-address—32-bit IP address
- nn—16-bit number

Command Default

None.

Command Modes

BGP autodiscovery configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure a bridge domain:

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# autodiscovery bgp
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-ad)#route-target 100:20
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

routed

To specify the bridge domain L3 interface, use the **routed** command in L2VPN bridge-group bridge-domain configuration submode. To revert, use the **no** form of the command.

routed interface BVI *BVI interface number*
no routed interface BVI *BVI interface number*

Syntax Description

interface	Bridge domain L3 interface.
BVI	Bridge-Group Virtual Interface.
BVI interface number	BVI interface number. The range is 1-65535.

Command Default

None

Command Modes

L2VPN bridge-group bridge-domain configuration submode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

The example shows how to specify the L3 bridge domain interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group bg1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bd1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# routed interface BVI 100
```

rpl

To specify one ring port on local node being RPL owner, neighbor or next-neighbor, use the **rpl** command in the Ethernet ring G.8032 instance configuration submode. To disable the port as RPL owner, neighbor or next-neighbor, use the **no** form of this command.

rpl {**port0** | **port1**} {**owner** | **neighbor** | **next-neighbor**}
no rpl {**port0** | **port1**} {**owner** | **neighbor** | **next-neighbor**}

Syntax Description

port0	Assigns port0 as RPL owner, neighbor or next-neighbor.
port1	Assigns port1 as RPL owner, neighbor or next-neighbor.
owner	Assigns port0 or port1 as RPL owner.
neighbor	Assigns port0 or port1 as neighbor.
next-neighbor	Assigns port0 or port1 as next neighbor.

Command Default

None

Command Modes

Ethernet ring G.8032 instance configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to assign port0 as neighbor:

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)# rpl port0 neighbor
RP/0/RSP0/CPU0:router(config-l2vpn-erp-instance)#
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show ethernet ring g8032

To display Ethernet ring G.8032 Protection data, use the **show ethernet ring g8032** command in the EXEC mode.

show ethernet ring g.8032 {**brief** *ring-name* | **profile** *ring-profile-name* | **statistics** | **status** {*ring-name* | **location** *location*} | **summary**}

Syntax Description

brief	Displays brief information on the G.8032 ethernet ring.
profile	Displays information about the G.8032 ethernet ring profile.
statistics	Displays the statistics of the G.8032 ethernet ring.
status	Displays the status of the G.8032 ethernet ring.
summary	Displays a summary of the G.8032 ethernet ring.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
vlan	read
interface	read
ethernet-services	read

This example shows the output of the **show ethernet ring g8032** command:

```
RP/0/RSP0/CPU0:router# show ethernet ring g8032 status


Ethernet ring Subring instance 1 is RPL Owner node in Protection state
  Port0: Bundle-Ether100 (Monitor: Bundle-Ether100)
         APS-Channel: Bundle-Ether100.1
         Status: RPL, faulty, blocked
         Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  Port1: GigabitEthernet0/0/0/38 (Monitor: GigabitEthernet0/0/0/38)
         APS-Channel: GigabitEthernet0/0/0/38.1
```

```
        Status: NonRPL
        Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  APS Level: 7
  Open APS ring topology
  Profile: timer-wtr (not defined)
    WTR interval: 5 minutes
    Guard interval: 500 milliseconds
    Hold-off interval: 0 seconds
    Revertive mode

Ethernet ring Subring-2 instance 1 is RPL Owner node in Idle state
  Port0: GigabitEthernet0/0/0/33 (Monitor: GigabitEthernet0/0/0/33)
        APS-Channel: GigabitEthernet0/0/0/33.1
        Status: RPL, blocked
        Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  Port1: GigabitEthernet0/0/0/3 (Monitor: GigabitEthernet0/0/0/3)
        APS-Channel: GigabitEthernet0/0/0/3.1
        Status: NonRPL
        Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  APS Level: 7
  Open APS ring topology
  Profile: timer-wtr (not defined)
    WTR interval: 5 minutes
    Guard interval: 500 milliseconds
    Hold-off interval: 0 seconds
    Revertive mode
RP/0/RSP0/CPU0:router#


RP/0/RSP0/CPU0:router# show ethernet ring g8032 brief
Wed Mar 16 07:14:28.719 UTC

  R: Interface is the RPL-link
  F: Interface is faulty
  B: Interface is blocked
 FS: Local forced switch
 MS: Local manual switch

RingName                          Inst NodeType  NodeState    Port0    Port1
-------------------------------------------------------------------------------
Subring                              1 Owner     Protection   R,F,B
Subring-2                            1 Owner     Idle         R,B
RP/0/RSP0/CPU0:F4-2-A9K#


RP/0/RSP0/CPU0:router# show ethernet ring g8032 summary
Wed Mar 16 07:14:52.419 UTC

Chassis Node Id 0026.982b.c6e7

States
------------------------------
  Init              0
  Idle              1
  Protection        1
  Manual Switch     0
  Forced Switch     0
  Pending           0
  --------------------------
  Total             2
RP/0/RSP0/CPU0:router#


RP/0/RSP0/CPU0:router# show ethernet ring g8032 statistics Subring instance 1
```

```
Statistics for Ethernet ring Subring instance 1
Local SF detected:
  Port0: 1
  Port1: 0

R-APS   Port0(Tx/Rx)                    Port1(Tx/Rx)
        Last Tx time                    Last Tx time
        Last Rx time                    Last Rx time
--------------------------------------------------------------------------------
NR    : 3/0                             0/0
        Tue Mar 15 04:41:00.964 UTC     Never
        Never                           Never
NR,RB : 0/0                             0/0
        Never                           Never
        Never                           Never
SF    : 19129/0                         19129/0
        Wed Mar 16 07:15:28.995 UTC     Wed Mar 16 07:15:28.774 UTC
        Never                           Never
MS    : 0/0                             0/0
        Never                           Never
        Never                           Never
FS    : 0/0                             0/0
        Never                           Never
        Never                           Never
EVENT : 0/0                             0/0
        Never                           Never
        Never                           Never

State           Last entry into state time
--------------------------------------------------------------------------------
Init          : Tue Mar 15 04:41:00.933 UTC
Idle          : Never
Protection    : Tue Mar 15 04:41:00.973 UTC
Manual Switch : Never
Forced Switch : Never
Pending       : Tue Mar 15 04:41:00.962 UTC
RP/0/RSP0/CPU0:router#


RP/0/RSP0/CPU0:router# show ethernet ring g8032 profile timer-wtr
Wed Mar 16 07:20:04.996 UTC

Ethernet ring profile name: timer-wtr
    WTR interval: 1 minutes
    Guard interval: 500 milliseconds
    Hold-off interval: 0 seconds
    Revertive mode
RP/0/RSP0/CPU0:router#
```

Related Commands

Command	Description
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show l2vpn bridge-domain (VPLS)

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
RP/0/RSP0/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 10.0.0.1, Multicast Group 225.1.1.1, UDP Port 4789
    Anycast VTEP 100.1.1.1, Anycast Multicast Group 224.10.10.1
    MAC learning: enabled
    Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
    MAC aging time: 300 s, Type: inactivity
    MAC limit: 4000, Action: none, Notification: syslog
    MAC limit reached: no
    MAC port down flush: enabled
    MAC Secure: disabled, Logging: disabled
    Split Horizon Group: none
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    DHCPv4 snooping: disabled
    IGMP Snooping: enabled
    IGMP Snooping profile: none
    MLD Snooping profile: none
    Storm Control: bridge-domain policer

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

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

```
RP/0/RSP0/CPU0:router# #show l2vpn bridge-domain
Tue Feb 23 20:21:56.758 PST
```

```
Bridge group: 189, bridge-domain: 189, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 2 (2 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/3.189, state: up, Static MAC addresses: 0
    Gi0/1/0/7.189, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
Bridge group: 190, bridge-domain: 190, id: 1, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 0 (0 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
  List of ACs:
  List of Access PWs:
  List of VFIs:
    VFI 190
      Neighbor 10.19.19.19 pw-id 190, state: up, Static MAC addresses: 0
Bridge group: 210, bridge-domain: 210, id: 2, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/7.210, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI 210
      Neighbor 10.19.19.19 pw-id 210, state: up, Static MAC addresses: 0
Bridge group: 211, bridge-domain: 211, id: 3, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/7.211, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI 211
      Neighbor 10.19.19.19 pw-id 211, state: up, Static MAC addresses: 0
Bridge group: 215, bridge-domain: 215, id: 4, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 2 (2 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/3.215, state: up, Static MAC addresses: 0
    Gi0/1/0/7.215, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI 215
      Neighbor 10.19.19.19 pw-id 215, state: up, Static MAC addresses: 0
Bridge group: 2130, bridge-domain: 2130, id: 5, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
  List of ACs:
    Gi0/1/0/7.2130, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI 2130
      Neighbor 10.19.19.19 pw-id 2130, state: up, Static MAC addresses: 0
```

This table describes the significant fields shown in the display.

Table 7: show l2vpn bridge-domain Command Field Descriptions

Field	Description
Bridge group	Name of bridge domain group is displayed.
bridge-domain	Name of bridge domain is displayed.
id	ID assigned to this bridge domain is displayed.
state	Current state of the bridge domain is displayed.
ShgId	ID for the default Split Horizon Group assigned to all attachment circuits and access pseudowires that are part of this bridge domain is displayed. **Note** Members of the special Split Horizon Group ID 0 forwards to other members of the same SPG.

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

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain bd-name bd1

Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
  List of ACs:
    Gi0/1/0/0, state: up, Static MAC addresses: 2, MSTi: 0 (unprotected)
  List of Access PWs:
  List of VFIs:
    VFI 1
      Neighbor 10.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
```

The following sample output shows brief information about the bridges:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain brief
Bridge Group/Bridge-Domain Name  ID    State      Num ACs/up     Num PWs/up
-------------------------------- ----- ---------- -------------- ------------
bg1/bd1                          0     up         1/1            0/0
bg1/bd2                          1     up         0/0            0/0
bg1/bd3                          2     up         0/0            0/0
```

This table describes the significant fields shown in the display.

Table 8: show l2vpn bridge-domain brief Command Field Descriptions

Field	Description
Bridge Group/Bridge-Domain Name	Bridge domain group name followed by the bridge domain name are displayed.
ID	ID assigned to this bridge domain is displayed.
State	Current state of the bridge domain is displayed.

Field	Description
Num ACs/up	Total number of attachment circuits that are up in this bridge domain is displayed.
Num PWs/up	Total number of pseudowires that are up in this bridge domain is displayed. The count includes both VFI pseudowires and access pseudowires.

The following sample output shows detailed information for IOS-XR releases 5.3.1 and earlier releases.

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

Bridge group: 210, bridge-domain: 210, id: 2, state: up, ShgId: 0, MSTi: 0
  MAC learning: enabled
  MAC withdraw: disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: no
  Security: disabled
  Split Horizon Group: none
  DHCPv4 snooping: disabled
  IGMP Snooping profile: none
  Bridge MTU: 9000
  Filter MAC addresses:
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
  List of ACs:
    AC: GigabitEthernet0/1/0/7.210, state is up
      Type VLAN; Num Ranges: 1
     vlan ranges: [100, 100]
      MTU 9008; XC ID 0x440007; interworking none; MSTi 0 (unprotected)
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: no
      Security: disabled
      Split Horizon Group: enabled
      DHCPv4 snooping: disabled
      IGMP Snooping profile: none
      Storm Control: disabled
      Static MAC addresses:
      Statistics:
        packet totals: receive 31645, send 6
        byte totals: receive 2405020, send 456
        Storm control drop counters:
          packet totals: broadcast 0, multicast 0, unknown unicast 0
          byte totals: broadcast 0, multicast 0, unknown unicast 0
  List of Access PWs:
  List of VFIs:
    VFI 210
      PW: neighbor 10.19.19.19, PW ID 210, state is up ( established )
        PW class not set, XC ID 0xfffc0004
        Encapsulation MPLS, protocol LDP
        PW type Ethernet, control word disabled, interworking none
        PW backup disable delay 0 sec
```

```
    Sequencing not set
            MPLS         Local                          Remote
      ------------ ------------------------------ -------------------------
      Label        16001                          16
      Group ID     0x2                            0x0
      Interface    210                            unknown
      MTU          9000                           9000
      Control word disabled                       disabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                     (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x6                           0x2
                   (router alert label)           (router alert label)         s
                   (TTL expiry)
      ------------ ------------------------------ -------------------------
    Create time: 13/04/1900 14:36:13 (17:46:22 ago)
    Last time status changed: 13/04/1900 15:37:03 (16:45:32 ago)
    MAC withdraw message: send 0 receive 0
    Static MAC addresses:
    Statistics:
      packet totals: receive 6, send 31655
      byte totals: receive 432, send 2279160
  IGMP Snooping profile: none
  VFI Statistics:
    drops: illegal VLAN 0, illegal length 0
```

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

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain detail
Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  MAC learning: enabled
  MAC withdraw: disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
  List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003

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

```
    VFI 1
      PW: neighbor 10.0.0.1, PW ID 1, state is up ( established )
        PW class mpls, XC ID 0xff000001
        Encapsulation MPLS, protocol LDP
        PW type Ethernet, control word disabled, interworking none
        PW backup disable delay 0 sec
        Sequencing not set
                MPLS         Local                          Remote
          ------------ ------------------------------ ----------
          Label        16003                          16003
          Group ID     0x0                            0x0
          Interface    1                              1
          MTU          1500                           1500
          Control word disabled                       disabled
          PW type      Ethernet                       Ethernet
          VCCV CV type 0x2                            0x2
                       (LSP ping verification)        (LSP ping verification)
          VCCV CC type 0x2                            0x2
                       (router alert label)           (router alert label)
          ------------ ------------------------------ ----------
        Create time: 12/03/2008 14:03:00 (17:17:30 ago)
        Last time status changed: 13/03/2008 05:57:58 (01:22:31 ago)
        MAC withdraw message: send 0 receive 0
        Static MAC addresses:

      VFI Statistics:
        drops: illegal VLAN 0, illegal length 0

Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-edge, I-SID: 1234
  Core-bridge: pbb-bd2
  MAC learning: enabled
  MAC withdraw: disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
List of PBBs:
    PBB Edge, state is up
      XC ID 0x2000001
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: yes
      Split Horizon Group: none
      DHCPv4 snooping: disabled
      IGMP Snooping profile:
      Storm Control: disabled
      Unknown-unicast-bmac: 666.777.888
      CMAC to BMAC Mapping Table:
         CMAC             |    BMAC
         -------------------------------------------------
         222.333.444      |    777.888.999
         333.444.555      |    888.999.111
```

```
      Statistics:
        packet totals: receive 3919680,send 9328
        byte totals: receive 305735040,send 15022146

 List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003



Bridge group: g2, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
  Type:  pbb-core
  Number of associated pbb-edge BDs: 1
  MAC learning: enabled
  MAC withdraw: disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:

ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
List of PBBs:
    PBB Core, state is up
      Vlan-id: 1; XC ID 0x2000001
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 600, Action: none, Notification: syslog
      MAC limit reached: no
      Security: disabled
      Split Horizon Group: none
      DHCPv4 snooping: profile foo
      IGMP Snooping profile:
      Storm Control: disabled

List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
```

```
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: yes
      Security: disabled
      DHCPv4 snooping: disabled
      Static MAC addresses:
        0000.0000.0000
        0001.0002.0003
```

This table describes the significant fields shown in the display.

Table 9: show l2vpn bridge-domain detail Command Field Descriptions

Field	Description
Bridge group	Name of bridge domain group is displayed.
bridge-domain	Name of bridge domain is displayed.
ID	ID assigned to this bridge domain is displayed.
state	Current state of the bridge domain is displayed.
ShgId	Split horizon group ID. This field is not used.
MSTi	ID for the Multiple Spanning Tree.
Split Horizon Group	Shows whether the AC is a member of the split horizon group for ACs. There is only one split horizon group for ACs per bridge domain. • Enabled—The port belongs to the split horizon group for ACs. • None—The port does not belong to the split horizon group for ACs.

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

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain group g1

Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
  List of ACs:
    Gi0/1/0/0, state: up, Static MAC addresses: 2, MSTi: 0 (unprotected)
  List of Access PWs:
  List of VFIs:
    VFI 1
      Neighbor 10.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
```

The following sample output shows display the filter information for the interface on the bridge domain for IOS-XR 5.3.1 and earlier releases:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain interface gigabitEthernet 0/1/0/0

Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
  List of ACs:
```

```
    Gi0/1/0/0, state: up, Static MAC addresses: 2, MSTi: 0 (unprotected)
```

The following sample output shows that the bridge domain contains the pseudowires to match the filter for the neighbor for IOS-XR 5.3.1 and earlier releases:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain neighbor 10.1.1.1

Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
  List of Access PWs:
  List of VFIs:
    VFI 1
      Neighbor 10.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
```

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

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

Number of groups: 1, bridge-domains: 2, Up: 2, Shutdown: 0
Default: 0, pbb-edge: 1, pbb-core: 1
Number of ACs: 1 Up: 1, Down: 0
Number of PWs: 0 Up: 0, Down: 0
```

This table describes the significant fields shown in the display.

Table 10: show l2vpn bridge-domain summary Command Field Descriptions

Field	Description
Number of groups	Number of configured bridge domain groups is displayed.
bridge-domains	Number of configured bridge domains is displayed.
Shutdown	Number of bridge domains that are in Shutdown state is displayed.
Number of ACs	Number of attachment circuits that are in Up state and Down state are displayed.
Number of PWs	Number of pseudowires that are in Up state and Down state are displayed. This includes the VFI pseudowire and the access pseudowire.

Related Commands

Command	Description
clear l2vpn bridge-domain (VPLS), on page 218	Clears the MAC addresses and restarts the bridge domains on the router.

show l2vpn ethernet ring g8032

To display an overview of the G.8032 ethernet ring configuration, use the **show l2vpn ethernet ring g8032** command in EXEC mode.

show l2vpn ethernet ring g8032 *[name]* [**brief** | **detail** | **instance** *ID* | **private**]

Syntax Description

name	Ethernet ring G.8032 name.
brief	Brief information about the G.8032 ethernet ring configuration.
detail	Information in detail about the G.8032 ethernet ring configuration.
instance*ID*	Instance number about the G.8032 ethernet ring configuration.
private	Private information about the G.8032 ethernet ring configuration.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read

Example

This example shows the output from the **show l2vpn ethernet ring g8032** command:

```
# show l2vpn ethernet ring g8032 foo instance 1
Ethernet ring g8032 foo
  Port0: GigabitEthernet0/1/2/0
  Port1: GigabitEthernet0/1/2/1
  Instance 1
     Inclusion-list vlan ids: 500-1000, 1017
     aps-channel
        port0: GigabitEthernet0/1/2/0.1
        port1: GigabitEthernet0/1/2/1.1


# show l2vpn ethernet ring g8032 foo instance 1 brief
```

```
Ring      instance  status
--------- --------  --------
Foo        1        resolved

# show l2vpn ethernet ring g8032 foo instance 1 detail
Ethernet ring g8032 foo
  Operating in Provider Bridge mode
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Exclusion-list vlan ids: 2000-2100, untagged
  Open-ring: no

  Instance 1
     Description: This_is_a_sample
     Profile    : none
     RPL        : none
     Inclusion-list vlan ids: 500-1000, 1017
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.1
        port1: GigabitEthernet0/1/2/1.1


# show l2vpn ethernet ring g8032 foo instance 1 private
Ethernet ring g8032 foo (task-id = cisco-support)
  Operating in Provider Bridge mode
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Exclusion-list vlan ids: 2000-2100, untagged
  Open-ring: no

  Instance 1
     Description: This_is_a_sample
     Profile    : none
     RPL        : none
     Inclusion-list vlan ids: 500-1000, 1017
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.1
        port1: GigabitEthernet0/1/2/1.1


   ethernet ring g8032 trace history [Num events: 6]
   ------------------------------------------------
   Time                 Event                     Sticky Many
   ====                 =====                     ====== ====
   05/18/2010 21:45:54 Create                     No     No
   05/18/2010 21:45:54 Resolved                   No     No
   05/18/2010 21:45:57 Create                     No     No
   05/18/2010 21:45:57 Modify                     No     No
   05/18/2010 21:45:57 Resolved                   No     No
   05/18/2010 21:45:57 Delete                     No     No
```

Related Commands

Command	Description
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show l2vpn forwarding bridge-domain (VPLS)

To display information on the bridge that is used by the forwarding layer, use the **show l2vpn forwarding bridge-domain** command in EXEC mode.

show l2vpn forwarding bridge-domain [*bridge-domain-name*] {**detail** | **hardware** {**egress** | **ingress**}} **location** *node-id*

Syntax Description

bridge-domain-name	(Optional) Name of a bridge domain.
detail	Displays all the detailed information on the attachment circuits and pseudowires.
hardware	Displays the hardware location entry.
egress	Reads information from the egress PSE.
ingress	Reads information from the ingress PSE.
location *node-id*	Displays the bridge-domain information for the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

For each bridge, you can display summary information about the number of bridge ports, number of MAC addresses, 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 for IOS-XR 5.3.1 and earlier releases:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain location 0/1/CPU0

Bridge-Domain Name               ID     Ports addr   Flooding Learning State
-------------------------------- ------ ----- ------ -------- -------- ---------
g1:bd1

Bridge-domain name: g1:bd1, id: 0, state: up
 MAC learning: enabled
 Flooding:
   Broadcast & Multicast: enabled
   Unknown unicast: enabled
 MAC aging time: 300 s, Type: inactivity
 MAC limit: 4000, Action: none, Notification: syslog
 MAC limit reached: yes
 Security: disabled
 DHCPv4 snooping: profile not known on this node
 Bridge MTU: 1500 bytes
 Number of bridge ports: 2
 Number of MAC addresses: 65536
 Multi-spanning tree instance: 0

  GigabitEthernet0/1/0/0, state: oper up
    Number of MAC: 32770
    Sent(Packets/Bytes): 0/21838568
    Received(Packets/Bytes): 5704781/444972918

  Nbor 10.0.0.1 pw-id 1
    Number of MAC: 32766
    Sent(Packets/Bytes): 0/0
    Received(Packets/Bytes): 5703987/444910986
            0      2     65536  Enabled  Enabled  UP
```

This table describes the significant fields shown in the display:

Table 11: show l2vpn forwarding bridge-domain Command Field Descriptions

Field	Description
Bridge-Domain Name	Name of bridge domain is displayed.
Bridge ID	ID assigned to this bridge domain is displayed.
Ports	Number of ports that are part of this bridge domain is displayed.
MAC Addr	Number of MAC addresses that are learned on this bridge domain is displayed.
Flooding	Flooding of packets are displayed if they are enabled on this bridge domain.
Learning	Learning of MAC addresses are displayed if they are enabled on this bridge domain.
State	Current state of the bridge domain is displayed.

Related Commands

Command	Description
clear l2vpn bridge-domain (VPLS), on page 218	Clears the MAC addresses and restarts the bridge domains on the router.

show l2vpn forwarding bridge-domain mac-address (VPLS)

To display the summary information for the MAC address, use the **show l2vpn forwarding bridge-domain mac-address** command in EXEC mode.

show l2vpn forwarding bridge-domain [*bridge-domain-name*] **mac-address** {*MAC-address* | **detail** | **hardware** {**egress** | **ingress**} | **interface** *type interface-path-id* | **neighbor** *address* **pw-id** *pw-id*} **location** *node-id*

Syntax Description

bridge-domain-name	(Optional) Name of a bridge domain.
MAC-address	MAC address.
detail	Displays detailed information for the MAC address.
hardware	Reads information from the hardware.
egress	Reads information from the egress PSE.
ingress	Reads information from the ingress PSE.
interface	Displays the match for the attachment circuit subinterface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
neighbor *address*	Displays the match for the neighbor IP address.
pw-id *pw-id*	Displays the match for the pseudowire ID.
location *node-id*	Displays the bridge-domain information for the MAC address of the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.0	This command was introduced.
Release 3.7.2	This command was introduced.
Release 3.8.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 location 0/1/CPU0
                                Bridge       MAC
Bridge-Domain Name              ID     Ports addr   Flooding Learning State
------------------------------- ------ ----- ------ -------- -------- ---------
g1:bd1                          0      2     65536  Enabled  Enabled  UP
```

The following sample output shows the list of MAC addresses that are learned on a specified bridge and summary information for the addresses:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
-------------------------------------------------------------------------------
0000.0000.0000 static  Gi0/1/0/0                  N/A        N/A
0000.0001.0101 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0102 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0103 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0104 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0105 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0106 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0107 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0108 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0109 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010a dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010b dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010c dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010d dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010e dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010f dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0110 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0111 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0112 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
....
```

The following sample output shows the MAC address on a specified interface on a specified bridge:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 mac-address 1.2.3 location
 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
-------------------------------------------------------------------------------
0001.0002.0003 static  Gi0/1/0/0                  N/A        N/A
```

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

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 mac-address hardware
```

```
egress location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
------------------------------------------------------------------------------
0000.0000.0000 static  Gi0/1/0/0                  N/A        N/A
0000.0001.0101 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0102 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0103 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0104 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0105 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0106 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0107 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0108 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0109 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.010a dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.010b dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.010c dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.010d dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.010e dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.010f dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0110 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0111 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0112 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0113 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
0000.0001.0114 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 24s
...
```

The following sample output shows the MAC addresses that are learned on a specified pseudowire on a specified bridge:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address neighbor 10.1.1.1
pw-id 1 location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
------------------------------------------------------------------------------
0000.0003.0101 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0102 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0103 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0104 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0105 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0106 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0107 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0108 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0109 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.010a dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.010b dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.010c dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.010d dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.010e dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.010f dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0110 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0111 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0112 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0113 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0114 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
0000.0003.0115 dynamic 10.1.1.1, 1                 0/1/CPU0   0d 0h 0m 30s
...
```

The following sample output shows the detailed information for MAC addresses that are learned on a specified interface and on specified bridge of a specified interface card. The sample output lists all the MAC addresses, the learned location, and the current age.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain g1:bd1 mac-address interface
gigabitEthernet 0/1/0/0 location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
-------------------------------------------------------------------------------
0000.0000.0000 static  Gi0/1/0/0                  N/A        N/A
0000.0001.0101 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0102 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0103 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0104 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0105 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0106 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0107 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0108 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0109 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.010a dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.010b dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.010c dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.010d dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.010e dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.010f dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0110 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0111 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0112 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0113 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s
0000.0001.0114 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 14s

RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address location 0/1/CPU0

Mac Address    Type    Learned from/Filtered on    LC learned Age
-------------------------------------------------------------------------------
0000.0000.0000 static  Gi0/1/0/0                  N/A        N/A
0000.0001.0101 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0102 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0103 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0104 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0105 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0106 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0107 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0108 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0109 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010a dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010b dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010c dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010d dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010e dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.010f dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0110 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0111 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
0000.0001.0112 dynamic Gi0/1/0/0                  0/1/CPU0   0d 0h 2m 22s
....
```

Related Commands

Command	Description
show l2vpn forwarding bridge-domain (VPLS), on page 296	Displays information on the bridge that is used by the forwarding layer.

show l2vpn forwarding ethernet ring g8032

To display an overview of the G.8032 ethernet ring configuration from L2Forwarding Information Base (L2FIB) process, use the **show l2vpn forwarding ethernet ring g8032** command in EXEC mode.

show l2vpn forwarding ethernet ring g8032 *name* [**detail** | **instance** *ID* | **location** | **private**]

Syntax Description

name	Ethernet ring G.8032 name.
detail	Information in detail about the G.8032 ethernet ring configuration.
instance*ID*	Instance number about the G.8032 ethernet ring configuration.
location	Location specified in the rack/slot/module notation.
private	Private information about the G.8032 ethernet ring configuration.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read

Example

This example shows the output from the **show l2vpn forwarding ethernet ring g8032** command:

```
# show l2vpn forwarding ethernet ring g8032 private location <r/s/i>
Ethernet ring g8032 foo (task-id = cisco-support)
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Open-ring: no
  TCN propagation: no
  Instance 1
     Profile    : none
     RPL        : none
     aps-channel
```

```
        port0: GigabitEthernet0/1/2/0.1, status: bound
        port1: GigabitEthernet0/1/2/1.1, status: unbound
  Instance 2
     Profile    : none
     RPL        : none
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.10, status: unbound
   ethernet ring g8032 trace history [Num events: 6]
   ------------------------------------------------
   Time                Event                     Sticky Many
   ====                =====                     ====== ====
   05/18/2010 21:45:54 Create                    No     No
   05/18/2010 21:45:57 Create                    No     No
   05/18/2010 21:45:57 Modify                    No     No
   05/18/2010 21:45:57 Delete                    No     No

# show l2vpn forwarding ethernet ring g8032 foo instance 1 detail location <r/s/i>
Ethernet ring g8032 foo
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Open-ring: no
  TCN propagation: no
  Instance 1
     Profile    : none
     RPL        : none
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.1, status: bound
        port1: GigabitEthernet0/1/2/1.1, status: unbound

# show l2vpn forwarding ethernet ring g8032 foo instance 1 private location <r/s/i>
Ethernet ring g8032 foo (task-id = cisco-support)
  Port0: GigabitEthernet0/1/2/0
     Monitor: none
  Port1: GigabitEthernet0/1/2/1
     Monitor: none
  Open-ring: no
  TCN propagation: no
  Instance 1
     Profile    : none
     RPL        : none
     aps-channel
        level: 7
        port0: GigabitEthernet0/1/2/0.1, status: bound
        port1: GigabitEthernet0/1/2/1.1, status: unbound

   ethernet ring g8032 instance trace history [Num events: 6]
   ----------------------------------------------------------
   Time                Event                     Sticky Many
   ====                =====                     ====== ====
   05/18/2010 21:45:54 Create                    No     No
   05/18/2010 21:45:57 Create                    No     No
   05/18/2010 21:45:57 Modify                    No     No
   05/18/2010 21:45:57 Delete                    No     No
```

Related Commands

Command	Description
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show l2vpn forwarding protection main-interface

To display an overview of the main interface or instance operational information from L2Forwarding Information Base (L2FIB), use the **show l2vpn forwarding protection main-interface** command in EXEC mode.

show l2vpn forwarding protection main-interface [*interface name*] [**detail** | **location** | **private**]

Syntax Description

interface name	Interface name of the Ethernet ring G.8032 name.
detail	Information in detail about the G.8032 ethernet ring configuration.
location	Brief information about the G.8032 ethernet ring configuration.
private	Private information about the G.8032 ethernet ring configuration.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read

Example

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

```
# show l2vpn forwarding protection main-interface location <r/s/i>
Main Interface ID               Instance   State
------------------------------- ---------- --------
GigabitEthernet0/0/0/0          1          forward
GigabitEthernet0/0/0/0          2          forward
GigabitEthernet0/0/0/1          1          forward
```

```
# show l2vpn forwarding protection main-interface detail location <r/s/i>
Main Interface ID                 Instance  State    # of subIntf
--------------------------------- --------  -------- -------------
GigabitEthernet0/0/0/0            1        forward   1
GigabitEthernet0/0/0/0            2        forward    3
GigabitEthernet0/0/0/1            1        forward    1


# show l2vpn forwarding protection main-interface private location <r/s/i>

Main Interface ID                 Instance State    # of subIntf
--------------------------------- -------- -------- ------------
GigabitEthernet0/0/0/0            1       forward   1

   Base info: version=0xaabbcc1c, flags=0x0, type=14, reserved=0
   Ifhandle: 0x20000040, cfg_instance: 1, Protected: no
```

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.

show l2vpn protection main-interface

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.0	This command was introduced.
Release 7.7.1	The command output was enhanced to include protection access gateway subtype indication `MST-AG`.

Usage Guidelines

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

Example

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

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

Main Interface ID              Subintf Count Protected  Blocked
------------------------------ ------------- ---------- ----------
```

```
GigabitEthernet0/0/0/0         1             None       No
   Instance : 0
      State         : FORWARDING
      Sub-Intf #    : 1
      Flush    #    : 0
       Sub-interfaces : GigabitEthernet0/0/0/0.4


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

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

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

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

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

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

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

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

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


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

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

Main Interface ID              # of subIntf Protected
```

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

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

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

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


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

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

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

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

Related Commands

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.

shutdown (Bridge Domain)

To shut down a bridge domain to bring the bridge and all attachment circuits and pseudowires under it to admin down state, use the **shutdown** command in L2VPN bridge group bridge domain configuration mode. To re-enable the bridge domain, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

By default, the bridge is not shutdown.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

When a bridge domain is disabled, all VFIs associated with the bridge domain are disabled. You can still attach or detach members to or from the bridge domain as well as the VFIs associated with the bridge domain.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to disable the bridge domain named bar:

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

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

shutdown (VFI)

To disable virtual forwarding interface (VFI), use the **shutdown** command in L2VPN bridge group bridge domain VFI configuration mode. To re-enable VFI, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

By default, the VFI is not shutdown.

Command Modes

L2VPN bridge group bridge domain VFI configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to disable VFI:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# shutdown
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 254	Configures the MPLS static labels and the static labels for the access pseudowire configuration.

Command	Description
neighbor (VPLS), on page 260	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).

signaling-protocol

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

signaling-protocol {**bgp** | **ldp**}
no signaling-protocol {**bgp** | **ldp**}

Syntax Description

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

Command Default

LDP signaling is enabled.

Command Modes

BGP autodiscovery configuration

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to enable signaling for BGP protocol:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EGroup
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain eastdomain
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi eastvfi
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# autodiscovery bgp
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-ad)#route-target 100:20
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-ad)#signaling-protocol bgp
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

split-horizon group

To add an AC to a split horizon group, use the **split-horizon group** command in L2VPN bridge group bridge domain attachment circuit configuration mode. To remove the AC from the group, use the **no** form of this command.

split-horizon group
no split-horizon group

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN bridge group bridge domain attachment circuit configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
l2vpn	Read, write

Examples

The following example adds an EFP under a GigabitEthernet interface to the AC split horizon group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group metroA
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain east
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet0/1/0/6.15
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# split-horizon group
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# commit
```

Related Commands

Command	Description
show l2vpn bridge-domain (VPLS), on page 283	Display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains.

static-address (VPLS)

To add static entries to the MAC address for filtering, use the **static-address** command in L2VPN bridge group bridge domain MAC configuration mode. To remove entries profiled by the combination of a specified entry information, use the **no** form of this command.

static-address *MAC-address* **drop**
no static-address *MAC-address* **drop**

Syntax Description

MAC-address	Static MAC address that is used to filter on the bridge domain.
drop	Drops all traffic that is going to the configured MAC address.

Command Default

No static MAC address is configured.

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add static MAC entries in L2VPN bridge group bridge domain MAC configuration mode. This entry causes all packets with destination MAC address 1.1.1 to be dropped.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# static-address 1.1.1 drop
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.

Command	Description
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.

static-mac-address (VPLS)

To configure the static MAC address to associate a remote MAC address with a pseudowire or any other bridge interface, use the **static-mac-address** command in the appropriate L2VPN bridge group bridge domain configuration submode. To disable this feature, use the **no** form of this command.

static-mac-address *MAC-address*
no static-mac-address *MAC-address*

Syntax Description

MAC-address	Static address to add to the MAC address.

Command Default

None

Command Modes

L2VPN bridge group bridge domain VFI pseudowire configuration

L2VPN bridge group bridge domain attachment circuit configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi model
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# static-mac-address 1.1.1
```

The following example shows how to associate a GigabitEthernet interface from a bridge domain to static MAC address 1.1.1:

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# static-mac-address 1.1.1
```

The following example shows how to associate an access pseudowire to static MAC address 2.2.2:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# neighbor 10.1.1.2 pw-id 2000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)# static-mac-address 2.2.2
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 254	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 260	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
vfi (VPLS), on page 328	Configures virtual forwarding interface (VFI) parameters.

tcn-propagation

To enable topology change notification (TCN) propagation, use the **tcn-propagation** command in the L2VPN configuration submode.

tcn-propagation

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

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

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

Related Commands

Command	Description
ethernet ring g8032, on page 225	Enables G.8032 ring mode and enters the G.8032 configuration submode.

time (VPLS)

To configure the maximum aging time, use the **time** command in L2VPN bridge group bridge domain MAC aging configuration mode. To disable this feature, use the **no** form of this command.

time *seconds*
no time *seconds*

Syntax Description

seconds	MAC address table entry maximum age. The range is from 300 to 30000 seconds. Aging time is counted from the last time that the switch saw the MAC address. The default value is 300 seconds.

Command Default

seconds: 300

Command Modes

L2VPN bridge group bridge domain MAC aging configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

If no packets are received from the MAC address for the duration of the maximum aging time, the dynamic MAC entry previously learned is removed from the forwarding table.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to increase the maximum aging time to 600 seconds. After 600 seconds of inactivity from a MAC address, the MAC address is removed form the forwarding table.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# time 600
```

Related Commands

Command	Description
aging (VPLS), on page 211	Enters the MAC aging configuration submode to set the aging parameters such as time and type.

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.
type (VPLS), on page 326	Configures the type for MAC address aging.

transport rsvp-te

To enable RSVP-TE as transport on a VFI and to enter L2VPN bridge group bridge domain VFI multicast P2MP RSVP - TE configuration mode, use the **transport rsvp-te** command in L2VPN bridge group bridge domain VFI multicast P2MP configuration mode. To return to P2MP mode, use the **no** form of this command.

transport rsvp-te [**attribute-set**]
no transport rsvp-te [**attribute-set**]

Syntax Description

[**attribute-set**]	Specifies the TE attribute set parameters.

Command Default

Command Modes

L2VPN bridge group bridge domain VFI multicast P2MP configuration

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enable RSVP-TE as transport on a VFI:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# multicast p2mp
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-p2mp)# transport rsvp-te
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-p2mp-te)#
```

Related Commands

Command	Description
multicast p2mp, on page 258	Configures point to multi-point pseudowire in a VFI.

Command	Description
vfi (VPLS), on page 328	Configures virtual forwarding interface (VFI) parameters.
bridge-domain (VPLS), on page 216	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

type (VPLS)

To configure the type for MAC address aging, use the **type** command in L2VPN bridge group bridge domain MAC aging configuration mode. To disable this feature, use the **no** form of this command.

type {**absolute** | **inactivity**}
no type {**absolute** | **inactivity**}

Syntax Description

absolute	Configures the absolute aging type.
inactivity	Configures the inactivity aging type.

Command Default

By default, the inactivity type is configured.

Command Modes

L2VPN bridge group bridge domain MAC aging configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

In general, the type is set to inactivity. With an inactivity type configuration, a MAC address is removed from the forwarding table after the MAC address is inactive for the configured aging time.

With an absolute type configuration, a MAC address is always removed from the forwarding table after the aging time has elapsed once it is initially learned.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the MAC address aging type to absolute for every member of the bridge domain named bar:

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# type absolute
```

Related Commands

Command	Description
aging (VPLS), on page 211	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.
time (VPLS), on page 322	Configures the maximum aging time.

vfi (VPLS)

To configure virtual forwarding interface (VFI) parameters and to enter L2VPN bridge group bridge domain VFI configuration mode, use the **vfi** command in L2VPN bridge group bridge domain configuration mode. To remove all configurations that are made under the specified VFI, use the **no** form of this command.

vfi *vfi-name*
no vfi *vfi-name*

Syntax Description

vfi-name	Name of the specified virtual forwarding interface.

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to create a VFI:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.

Command	Description
l2vpn, on page 92	Enters L2VPN configuration mode.
mpls static label (VPLS), on page 254	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
neighbor (VPLS), on page 260	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).

withdraw (VPLS)

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

withdraw {**access-pw disable** | **disable**}
no withdraw {**access-pw disable** | **disable** }

Syntax Description

access-pw disable	Disables the sending of MAC withdraw messages to access pseudowires.
disable	Disables MAC address withdrawal.

Command Default

By default, MAC address withdrawal is enabled.

Command Modes

L2VPN bridge group bridge domain MAC configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.0.0	The **access-pw disable** keyword was added.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable disable MAC withdrawal:

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

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

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

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-mac)# withdraw access-pw disable
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.
mac (VPLS), on page 245	Enters L2VPN bridge group bridge domain MAC configuration mode.



EVPN Commands

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

For detailed information about EVPN concepts, configuration tasks, and examples, see the *EVPN Features* module in the *L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers*.

- access-signal out-of-service, on page 334
- access-signal, on page 335
- advertise gateway-ip-disable, on page 336
- advertise-mac, on page 337
- clear l2route evpn ipv4 , on page 338
- clear l2route evpn ipv6 , on page 339
- clear l2route evpn mac , on page 340
- evpn, on page 341
- evpn evi, on page 342
- evpn evi multicast source-connected, on page 343
- ethernet-segment, on page 345
- ethernet-segment (evpn) , on page 346
- implicit-import, on page 347
- interface (EVPN), on page 348
- l2vpn evpn, on page 350
- mac-flush, on page 352
- mpls static label (EVPN ELAN), on page 354
- mpls static label (EVPN VPWS), on page 355
- neighbor evpn, on page 356
- non-revertive, on page 357
- revert, on page 358
- route-target, on page 360
- set advertise-evpn-gw-ip , on page 362
- service-carving, on page 363
- show evpn ethernet-segment, on page 365
- show evpn summary, on page 368
- show evpn evi, on page 370
- show evpn internal-label, on page 374
- weight, on page 376

access-signal out-of-service

To override the default signal sent to bring down the AC and to transition the interface to Out-of-Service (OOS) state, use the **access-signal out-of-service** command in the EVPN interface configuration mode. To return to the default behavior, use the **no** form of this command.

access-signal out-of-service

Command Default

None

Command Modes

EVPN interface configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Starting from Cisco IOS XR Release 7.10.1, the EVPN port-active configuration supports hot standby where all the main and subinterfaces up in a Standby node. To revert to the previous behavior of transitioning through the OOS state, use this command.

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows how to configure the access signal mode to enable the OOS functionality.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 01.00.01.00.01.09.01.00.09
Router(config-evpn-ac-es)# load-balancing-mode port-active
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# access-signal out-of-service
Router(config-evpn-ac)# commit
```

access-signal

To configure control signaling messages in access circuits, use the **access-signal** command in the EVPN configuration mode.

access-signal [bundle-down | out-of-service]

Syntax Description

bundle-down	Initiates Access Signal Bundle Down.
out-of-service	Initiates Access signal bundle out of service.

Command Default

None.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to configure **access-signal** command in EVPN configuration mode:

```
RP/0/RP0/CPU0:R1#config
RP/0/RP0/CPU0:R1(config)#evpn
RP/0/RP0/CPU0:R1(config-evpn)#interface Bundle-Ether 1
RP/0/RP0/CPU0:R1(config-evpn-ac)#access-signal bundle-down
```

advertise gateway-ip-disable

To disable advertisement of non-zero EVPN gateway IP address, use the **advertise gateway-ip-disable** command in the EVPN address-family configuration mode.

advertise gateway-ip-disable

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

EVPN address-family configuration mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to disable advertisement of non-zero EVPN gateway IP address:

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.10.10.10
Router(config-bgp-nbr)# remote-as 200
Router(config-bgp-nbr)# update-source Loopback 0
Router(config-bgp-nbr)# address-family l2vpn evpn
Router(config-bgp-nbr-af)# advertise gateway-ip-disable
Router(config-bgp-nbr-af)# commit
```

advertise-mac

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

advertise-mac

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EVPN

Command History

Release	Modification
Release 6.2.1	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.

The following example shows how to advertise local MAC.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 1
RP/0/RSP0/CPU0:router(config-evpn-evi)# bgp
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# table-policy spp-basic-6
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# route-target import 100:6005
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# route-target export 100:6005
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# exit
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac
```

clear l2route evpn ipv4

To clear either duplicate or frozen flags, or both, from EVPN MAC-IPv4 routes and re-enable local route learning for the corresponding IPv4 addresses, use **clear l2route evpn ipv4** command in EXEC mode.

clear l2route evpn ipv4 { *ipv4-address* } | **all** [**evi** *evi*] **frozen-flag**

Syntax Description

mac *mac-address*	Clears the route for the specified IPv4 address.
all	Clears all EVPN MAC-IPv4 routes that are marked as duplicate or permanently frozen.
evi *evi*	Clears EVPN MAC -IPv4 routes for the specified topology only.
frozen-flag	Clears either duplicate or frozen flag for the MAC-IPv4 routes that are identified by the specified options.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to clear duplicate or frozen flags, or both from EVPN MAC-IPv4 routes:

```
Router# clear l2route evpn ipv4 192.0.2.1 evi 1 frozen-flag
```

clear l2route evpn ipv6

To clear either duplicate or frozen flags, or both, from EVPN MAC-IPv6 routes and re-enable local route learning for the corresponding IPv6 addresses, use **clear l2route evpn ipv6** command in EXEC mode.

clear l2route evpn ipv6 { *ipv6-address* } | **all** [**evi** *evi*] **frozen-flag**

Syntax Description

mac *mac-address*	Clears the route for the specified IPv6 address.
all	Clears all EVPN MAC-IPv6 routes that are marked as duplicate or permanently frozen.
evi *evi*	Clears EVPN MAC-IPv6 routes for the specified topology only.
frozen-flag	Clear duplicate or frozen flag for the MAC-IPv6 routes that are identified by the specified options.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to clear either duplicate or frozen flags, or both, from EVPN MAC-IPv6 routes:

```
Router# clear l2route evpn IPv6 2001:DB8::1 evi 1 frozen-flag
```

clear l2route evpn mac

To clear either duplicate or frozen flags, or both, from EVPN MAC routes and re-enable local route learning for the corresponding MAC addresses, use **clear l2route evpn mac** command in EXEC mode.

clear l2route evpn mac {*mac-address*} | **all** [**evi** *evi*] **frozen-flag**

Syntax Description

mac *mac-address*	Clears the route for the specified MAC address.
all	Clears all EVPN MAC routes that are marked as duplicate or permanently frozen.
evi *evi*	Clears EVPN MAC routes for the specified topology only.
frozen-flag	Clears duplicate or frozen flag for the MAC routes that are identified by the specified options.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to clear duplicate or frozen flags, or both, from EVPN MAC routes:

```
Router# clear l2route evpn mac 0.12.3456 evi 1 frozen-flag
```

evpn

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

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

Syntax Description

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

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.2	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
l2vpn	read, write

Example

This example shows how to enter the EVPN configuration mode:

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

evpn evi

To configure EVPN instance (EVI) use the **evpn evi** command in the global configuration mode. To remove the configuration, use the **no** form of this command.

evpn evi *evi-id*

Syntax Description

evi-id	Specifies the Ethernet VPN ID to set. Before Release 25.2.1, The range is from 1 to 65534. From Release 25.2.1, The range is from 1 to 16777215.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Release 25.2.1	Extending the Ethernet VPN ID range to 16777215.
Release 6.6.3	This command was introduced.

Usage Guidelines

The EVI is represented by the virtual network identifier (VNI). An EVI represents a VPN on a PE router. It serves the same role of an IP VPN Routing and Forwarding (VRF), and EVIs are assigned to import/export Route Targets. This command configures the EVI and enters the EVPN Instance configuration mode, where you can configure EVPN settings.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to configure EVPN EVI that enters the EVPN Instance configuration mode.

```
Router# configure
Router(config)# evpn evi 10
Router((config-evpn-instance)#
```

evpn evi multicast source-connected

To configure EVPN multicast instance with a locally connected multicast source, use the **evpn evi** *evi-id* **multicast source-connected** command in the Global configuration mode or EVPN instance configuration mode. To remove the configuration, use the **no** form of this command.

evpn evi *evi-id* [**multicast**] [**source-connected**]

Syntax Description

evi-id	Specifies the Ethernet VPN ID to set. The range is from 1 to 65534.
multicast	(Optional) Configures EVPN instance multicast.
source-connected	(Optional) Connects multicast traffic source.

Command Default

None.

Command Modes

Global configuration

EVPN instance configuration mode

Command History

Release	Modification
Release 6.6.3	This command was introduced.
Release 24.1.1	This command is deprecated

Usage Guidelines

This command is used in all-active dual-homed PE scenarios with BVI interfaces and host-routing for EVPN enabled networks.

This command installs an IPv4 or IPv6 host route in the routing table when a locally connected multicast source is available. This ensures that the Protocol Independent Multicast (PIM) has correct Reverse Path Forwarding (RPF) towards the local source and not to the EVPN-injected host route of the other PE.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to configure a multicast instance in global configuration mode.

```
Router# configure
Router(config)# evpn evi 10 multicast source-connected
Router(config)#
```

This example shows how to configure a multicast instance in EVPN Instance configuration mode.

```
Router# configure
Router(config)# evpn evi 10
Router(config-evpn-instance)# multicast source-connected
Router(config-evpn-instance)#
```

ethernet-segment

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

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

Syntax Description

backbone-source-mac	Specifies Backbone Source MAC.
identifier	Specifies Ethernet Segment Identifier.
load-balancing-mode	Specifies load balancing mode.
service-carving	Specifies service carving.

Command Default

None.

Command Modes

EVPN interface configuration

Command History

Release	Modification
Release 4.3.2	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
l2vpn	read, write

This example shows how to enter the EVPN interface ethernet segment configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# interface bundle-ether 1
RP/0/RSP0/CPU0:router(config-evpn-ac)# ethernet-segment
RP/0/RSP0/CPU0:router(config-evpn-ac-es)#
```

ethernet-segment (evpn)

To disable ESI auto-generation value for LACP ESI type 1, use the **ethernet-segment** command in the EVPN configuration mode. To enable ESI auto-generation, use the **no** form of this command.

ethernet-segmenttype 1 auto-generation-disable
no ethernet-segmenttype 1 auto-generation-disable

Syntax Description

type 1	Specifies LACP ESI-auto-generation for ESI type 1.
auto-generation-disable	Disables ESI auto-generation.

Command Default

By default, EVPN auto-generates an ESI value for the bundle interfaces by retrieving LACP information.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

This command allows mLACP to decide to either forward or stop EVPN multipath resolution on remote ESI.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to disable auto-generation ESI type 1:

```
Router# configure
Router(config)# evpn
Router(config-evpn)#ethernet-segment
Router(config-evpn-es)#type 1 auto-generation-disable
```

implicit-import

To import EVPN routes in BGP routing table, use **implicit-import** command in the EVPN configuration mode.

implicit-import

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to configure **implicit-import** command in EVPN configuration mode.

```
RP/0/RP0/CPU0:R1#config
RP/0/RP0/CPU0:R1(config)#evpn
RP/0/RP0/CPU0:R1(config-evpn)#evi 1
RP/0/RP0/CPU0:R1(config-evpn-instance)#bgp
RP/0/RP0/CPU0:R1(config-evpn-instance-bgp)#implicit-import
```

interface (EVPN)

To enter the physical or virtual interface configuration mode, use the **interface** command in the EVPN configuration mode. To return to the EVPN configuration mode, use the **no** form of this command.

interface *type interface path-id*
no interface *type interface path-id*

Syntax Description

type	Specifies the following interface types connected to the CE device: • Physical ethernet interface • Bundle ethernet For more information about the syntax for the router, use the question mark (**?**) online help function.
interface path-id	Physical or virtual interface name. The range for the bundle name is from 1 to 65535. **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

EVPN configuration mode

Command History

Release	Modification
Release 4.3.2	This command was introduced.
Release 7.3.1	The **PW-Ether** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To specify a physical interface, the notation for the *interface-path-id* is *rack/slot/module/port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the line card.

- *module*: Module number. A physical layer interface module (PLIM) is always 0.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enter the EVPN Interface configuration mode for bundle-ether 1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# interface bundle-ether 1
RP/0/RSP0/CPU0:router(config-evpn-ac)#
```

Related Commands

Command	Description
evpn, on page 341	Enters EVPN configuration mode.
ethernet-segment, on page 345	Enters EVPN interface ethernet segment configuration mode.

l2vpn evpn

To execute EVPN commands in L2VPN mode, use the **l2vpn evpn** command in the EXEC mode.

l2vpn evpn { **compute-hrw neighbor** *neighbor-ip-address* **esi** *esi-value* **service-id** *evi-value* | **ethernet-segment interface** *interface-name* **revert** | **ethernet-segment interface** *interface-name* **pref-switchover** }

Syntax Description

compute-hrw neighbor *neighbor-ip-address* **esi** *esi-value* **service-id***evi-value*	Generates Highest Random Weight (HRW) for a PE, which would be used during the DF election.
ethernet-segment interface *interface-name* **revert**	Disables the non-revertive mode and returns to the revertive mode of DF election.
ethernet-segment interface *interface-name* **pref-switchover**	Initiates an immediate switchover of the Designated Forwarder (DF) on the specified bundle service, swapping the DF role between the active router and the standby router.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 25.2.1	The **ethernet-segment interface** *interface-name* **pref-switchover** keyword was added.
Release 24.1.1	The **ethernet-segment interface** *interface-name* **revert** keyword was added.
Release 6.0.1	This command was introduced.

Usage Guidelines

For ethernet-segment interface *interface-name* pref-switchover command:

- Use the **l2vpn evpn ethernet-segment interface***interface-name* **pref-switchover** command to initiate the switchover mechanism only if you cannot manually configure a new weight on the router.
- If you have access to the router configuration, manually updating the Ethernet Segment (ES) weight is a more effective way to manage the DF role than using the **l2vpn evpn ethernet-segment interface***interface-name* **pref-switchover** command.
- A standby PE router must be available to perform a switchover operation. If there is no standby PE router, the IOS XR software performs these operations:
  1. Ignores the **l2vpn evpn ethernet-segment interface***interface-name* **pref-switchover** command.
  2. No DF election occurs and the current active PE router remains active.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows configuration to compute HRW.

```
Router# l2vpn evpn compute-hrw neighbor 10.1.1.1 esi 11.1111.1111.0011.1111 service-id 10
```

This example shows how to initiate an immediate EVPN port-active manual switchover of the DF on the specified bundle service, swapping the DF role between the active router and the standby router.

```
Router# l2vpn evpn ethernet-segment interface Bundle-Ether1 pref-switchover
```

This example shows how to disable the non-revertive mode of DF election.

```
Router# l2vpn evpn ethernet-segment interface Bundle-Ether1 revert
```

This example shows how to revert the manual switchover mechanism and switch the DF role back to the previous active router.

- On the previously active router, you can run **l2vpn evpn ethernet-segment interface***interface-name* **revert** command.

  ```
  Router# l2vpn evpn ethernet-segment interface Bundle-Ether1 revert
  ```

- Optionally, on the current active router, you can run **l2vpn evpn ethernet-segment interface***interface-name* **pref-switchover** command.

  ```
  Router# l2vpn evpn ethernet-segment interface Bundle-Ether10 pref-switchover
  ```

mac-flush

To perform a MAC flush on an Ethernet-segment, use the **mac-flush** command in the EVPN interface configuration mode. To disable the MAC flush setting, use the **no** form of this command.

mac-flush mvrp

Starting from Cisco IOS XR Release 7.11.2, the command has been replaced as follows:

mac-flush-message { **mvrp** | **disable** }

Syntax Description

mvrp	Specifies the MAC flush over MVRP.
disable	Disables the MAC flush messages.

Command Default

STP-TCN

Command Modes

EVPN interface configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.
Release 7.11.2	This command was replaced by the **mac-flush-message** command. The keyword **disable** was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to perform the MAC flush over MVRP on an Ethernet segment:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 36.37.00.00.00.00.00.11.00
Router(config-evpn-ac-es)#exit
Router(config-evpn-ac)# mac-flush mvrp
Router(config-evpn-ac)#
```

This example shows how to perform the MAC flush over MVRP on an Ethernet segment, starting from release 7.11.2:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 36.37.00.00.00.00.00.11.00
Router(config-evpn-ac-es)#exit
Router(config-evpn-ac)# mac-flush-message mvrp
Router(config-evpn-ac)#
```

This example shows how to disable the MAC flush messages on an Ethernet segment:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 36.37.00.00.00.00.00.11.00
Router(config-evpn-ac-es)#load-balancing-mode single-active
Router(config-evpn-ac-es)#exit
Router(config-evpn-ac)# mac-flush-message disable
Router(config-evpn-ac)#
```

mpls static label (EVPN ELAN)

To configure the MPLS static labels for unicast IP traffic, use the **mpls static label** command in EVPN EVI configuration mode.

mpls static label unicast *label*

Syntax Description

unicast *label*	Configures a static MPLS label for unicast IP traffic. Range is 16 to 1,048,575.

Command Default

None

Command Modes

EVPN EVI configuration

Command History

Release	Modification
Release 25.3.1	This command was introduced.

Usage Guidelines

Use static MPLS labels within the range of 16 to 15,000 to avoid conflicts with existing dynamic labels and the default Segment Routing Local Block (SRLB) range of 15,000 to 15,999. For more information, see About the Segment Routing Local Block in the *Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configures a static MPLS label for unicast IP traffic:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 1001
Router(config-evpn-evi)# advertise-mac
Router(config-evpn-evi)# mpls static label unicast 55555
```

mpls static label (EVPN VPWS)

To configure the MPLS static labels for EVPN VPWS, use the **mpls static label** command in L2VPN cross-connect P2P EVPN EVI configuration mode.

mpls static label local *label*

Syntax Description

local *label*	Configures a local EVPN EVI label. Range is 16 to 1,048,575.

Command Default

None

Command Modes

L2VPN cross-connect P2P EVPN EVI configuration

Command History

Release	Modification
Release 25.3.1	This command was introduced.

Usage Guidelines

Use static MPLS labels within the range of 16 to 15,000 to avoid conflicts with existing dynamic labels and the default Segment Routing Local Block (SRLB) range of 15,000 to 15,999. For more information, see About the Segment Routing Local Block in the *Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configures a static MPLS label for EVPN VPWS in L2VPN cross-connect P2P EVPN EVI configuration mode:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group g1
Router(config-l2vpn-xc)# p2p p2p1
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 1 service 1
Router(config-l2vpn-xc-p2p-evpn-instance)# mpls static label local 55555
```

neighbor evpn

To enable EVPN-VPWS endpoint on the p2p cross-connect, use the **neighbor evpn** command in the p2p configuration submode.

```
neighbor evpn evi vpn-id service { service-id | vlan-aware } target ac-id
```

Syntax Description

evi *vpn-id*	Virtual Private Network Identifier where this p2p xconnect is setup.
target *ac-id*	Specifies the targeted remote attachment circuit id of the EVPN.
vlan-aware	Specifies the vlan-aware service.

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 6.1.21	This command was introduced.
Release 7.11.1	The **vlan-aware** keyword was added.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

The following example shows how to enable EVPN-VPWS endpoint on the p2p cross-connect.

```
Router# configurerouter# interface TenGigE0/1/0/12
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group xc1
Router(config-l2vpn-xc)# p2p vpws
Router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 100 target 80
```

The following example shows how to configure vlan-aware PW Head end:

```
Router(config)#l2vpn
Router(config-l2vpn)#xconnect group evpn-headend
Router(config-l2vpn-xc)#p2p headend-va-1002
Router(config-l2vpn-xc-p2p)#interface PW-Ether 1002
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 1002 service vlan-aware
Router(config-l2vpn-xc-p2p)#root
```

non-revertive

To enable the non-revertive mode of DF election, use the **non-revertive** command in the EVPN ethernet segment service carving configuration mode.

non-revertive

Command Default

None

Command Modes

EVPN interface Ethernet segment service carving configuration mode

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

You can enable the non-revertive mode only on preference-based DF election. It is recommended to configure the non-revertive mode on all the nodes in the network.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enable non-revertive mode:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 01.11.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode port-active
Router(config-evpn-ac-es)# service-carving preference-based
Router(config-evpn-ac-es-sc-pref)# non-revertive
Router(config-evpn-ac-es-sc-pref)# weight 100
Router(config-evpn-ac-es-sc-pref)# commit
```

revert

To set a timer to switchover from non-revertive mode to revertive mode of DF election, use the **revert** *timer* command in the EVPN configuration mode or EVPN interface configuration mode.

revert *timer*

Syntax Description

timer	Specify the time interval for the revert timer in seconds. The range is 0 to 3600.

Command Default

None

Command Modes

- EVPN configuration mode
- EVPN interface configuration mode

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows revert timer configuration for a specific interface:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 01.11.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode port-active
Router(config-evpn-ac-es)# service-carving preference-based
Router(config-evpn-ac-es-sc-pref)# non-revertive
Router(config-evpn-ac-es-sc-pref)# weight 100
Router(config-evpn-ac-es-sc-pref)# exit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# timers
Router(config-evpn-ac-timers)# revert 300
Router(config-evpn-ac-es)# commit
```

This example shows global configuration for revert timer:

```
Router# configure
```

```
Router(config)# evpn
Router(config-evpn)# timers
Router(config-evpn-timers)# revert 300
Router(config-evpn-timers)# commit
```

route-target

To specify a route target for the VFI, use the **route-target** command in the BGP autodiscovery mode. To return to the default value, use the **no** form of this command.

route-target {*as-number:nn* *ip-address:nn* }
no route-target {*as-number:nn* *ip-address:nn* }

Syntax Description

as-number:nn	Autonomous system (AS) number of the route distinguisher. • as-number—16-bit AS number Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535. • nn—32-bit number
ip-address:nn	IP address of the route distinguisher. • ip-address—32-bit IP address • nn—16-bit number

Command Default

None.

Command Modes

BGP autodiscovery configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure a bridge domain:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EGroup
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain eastdomain
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# vfi eastvfi
```

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi)# autodiscovery bgp
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-vfi-ad)#route-target 100:20
```

Related Commands

Command	Description
bridge-domain (VPLS), on page 216	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 217	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 92	Enters L2VPN configuration mode.

set advertise-evpn-gw-ip

To advertise the EVPN gateway IP address as a next-hop IP address,, use the **set advertise-evpn-gw-ip** command in the route-policy configuration mode.

set advertise-evpn-gw-ip { **A.B.C.D** | **X:X::X** | **parameter** | **use-next-hop** }

Syntax Description

A.B.C.D	Specify an IPv4 address.
X:X::X	Specify an IPv6 address.
parameter	Identifier specified in the format: '$' followed by alphanumeric. characters
use-next-hop	Set advertise EVPN gateway IP as next-hop IP address.

Command Default

None

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
route-policy	read, write

Example

This example shows how to configure EVPN gateway IP address as a next-hop IP address:

```
Router(config)# route-policy gw
Router(config-rpl)# set advertise-evpn-gw-ip use-next-hop
Router(config-rpl)# end-policy
Router(config)# vrf VRF1
Router(config-vrf)# address-family ipv4 unicast
Router(config-vrf-af)# import route-target
Router(config-vrf-import-rt)# 10:10
Router(config-vrf-import-rt)# exit
Router(config-vrf-af)# export route-policy gw
Router(config-vrf-af)# export route-target
Router(config-vrf-export-rt)# 10:10
Router(config-vrf-export-rt)#commit
```

service-carving

To specify a list of service identifiers as active and standby services, use the **service-carving** command in the EVPN Ethernet segment configuration mode.

service-carving { **manual** [**primary** *service-id-range* **secondary** *service-id-range*] } | { **preference-based** [**access-driven** | **weight** *preference-df-weight* | **srg-driven** }]

Syntax Description

manual	Specifies service identifiers or EVI-list services manually.
primary	Specifies the primary services list.
secondary	Specifies the secondary services list.
service-id-range	Specifies the services list notation in the range 100, 201-300, 401. The range is within 256 to 16777214.
preference-based	Specifies preference-based service carving.
access-driven	Specifies acess-driven DF election.
weight	Specifies the preference value.
preference-df-weight	Specifies the preference DF weight. The range is from 0 to 65535 unless **access-driven** is configured, in which case it will be 0 to 32767. Default is 32767 when not configured.
srg-driven	Enables the Subscriber Redundancy Group, BNG DF Election.

Command Default

Automatic service carving

Command Modes

EVPN interface Ethernet segment configuration mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.
Release 7.3.1	The follwing keywords are added: • **preference-based** • **access-driven**
Release 7.11.1	The **srg-driven** keyword was added.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to specify a list of service identifiers as active and standby services:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)# ethernet segment
Router(config-evpn-ac-es)# service-carving manual primary 201-300 secondary 400-500
Router(config-evpn-ac-es)# commit
```

This example shows how to specify EVPN access-driven DF election:

```
Router#configure
Router(config)#evpn
Router(config-evpn)#interface Bundle-Ether1
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 01.11.00.00.00.00.00.00.01
Router(config-evpn-ac-es)#load-balancing-mode port-active
Router(config-evpn-ac-es)#service-carving preference-based
Router(config-evpn-ac-es-sc-pref)#weight 100
Router(config-evpn-ac-es-sc-pref)#access-driven
Router(config-evpn-ac-es-sc-pref)#commit
```

This example shows how to enable BNG SRG driven DF election for EVPN:

```
Router#configure
Router(config)#evpn
Router(config-evpn)#interface PW-Ether1002
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 00.10.02.00.00.00.00.10.02
Router(config-evpn-ac-es)#service-carving preference-based
Router(config-evpn-ac-es-sc-pref)# srg-driven
Router(config-evpn-ac-es-sc-pref)#commit
Router(config-evpn-ac-es-sc-pref)#root
```

show evpn ethernet-segment

To display the EVPN Ethernet segment information, use the **show evpn ethernet-segment** command in the EXEC mode.

show evpn ethernet-segment[**detail** | **esi** | **interface** | **location** | **private** | **standby**]

Syntax Description

detail	Displays detailed information.
esi	Filters by Ethernet Segment identifier.
interface	Filters by interface name.
location	Displays location specific information.
private	Displays private information.
standby	Displays standby node specific information.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.2	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
l2vpn	read

Example

This sample output shows the EVPN Ethernet segment with interface filter:

```
RP/0/RSP0/CPU0:router#show evpn ethernet-segment interface gigabitethernet 0/3/0/0 detail
Ethernet Segment Id      Interface      Nexthops
------------------------ -------------- ----------------------------------------
0210.0300.9e00.0210.0000 Gi0/3/0/0      1.100.100.100
                                        2.100.100.100
be01.0300.be01.ce00.0001 BE1            1.100.100.100
                                        2.100.100.100
be02.0300.be02.0101.0002 BE2            1.100.100.100
                                        2.100.100.100
```

```
N/A                     Gi0/3/0/3      N/A
```

This sample output shows the EVPN Ethernet segment detailed information:

```
RP/0/RSP0/CPU0:router#show evpn ethernet-segment detail
Tue Jun 25 14:17:09.610 EDT
Legend:
  A- PBB-EVPN load-balancing mode and Access Protection incompatible,
  B- no Bridge Ports PBB-EVPN enabled,
  C- Backbone Source MAC missing,
  E- ESI missing,
  H- Interface handle missing,
  I- Interface name missing,
  M- Interface in Down state,
  O- BGP End of Download missing,
  P- Interface already Access Protected,
  Pf-Interface forced single-homed,
  R- BGP RID not received,
  S- Interface in redundancy standby state,
  X- ESI-extracted MAC Conflict

Ethernet Segment Id      Interface      Nexthops
------------------------ -------------- ----------------------------------------
0210.0300.9e00.0210.0000 Gi0/3/0/0      1.100.100.100
                                        2.100.100.100
  ES to BGP Gates   : Ready
  ES to L2FIB Gates : Ready
  Main port         :
     Interface name : GigabitEthernet0/3/0/0
     IfHandle       : 0x1800300
     State          : Up
     Redundancy     : Not Defined
  Source MAC        : 0001.ed9e.0001 (PBB BSA)
  Topology          :
     Operational    : MHN
     Configured     : A/A per service (default)
  Primary Services  : Auto-selection
  Secondary Services: Auto-selection
  Service Carving Results:
     Bridge ports   : 3
     Elected        : 0
     Not Elected    : 3
          I-Sid NE  :  1450101, 1650205, 1850309
  MAC Flushing mode : STP-TCN
  Peering timer     : 45 sec [not running]
  Recovery timer    : 20 sec [not running]
  Flushagain timer  : 60 sec

be01.0300.be01.ce00.0001 BE1            1.100.100.100
                                        2.100.100.100
  ES to BGP Gates   : Ready
  ES to L2FIB Gates : Ready
  Main port         :
     Interface name : Bundle-Ether1
     IfHandle       : 0x000480
     State          : Up
     Redundancy     : Active
  Source MAC        : 0024.be01.ce00 (Local)
  Topology          :
     Operational    : MHN
     Configured     : A/A per flow (default)
  Primary Services  : Auto-selection
  Secondary Services: Auto-selection
```

```
Service Carving Results:
   Bridge ports   : 3
   Elected        : 3
        I-Sid E   :  1450102, 1650206, 1850310
   Not Elected    : 0
MAC Flushing mode : STP-TCN
Peering timer     : 45 sec [not running]
Recovery timer    : 20 sec [not running]
Flushagain timer  : 60 sec
```

Related Commands

Command	Description
evpn, on page 341	Enters EVPN configuration mode.
ethernet-segment, on page 345	Enters EVPN interface ethernet segment configuration mode.

show evpn summary

To display the EVPN summary, use the **show evpn summary** command in the EXEC mode.

show evpn summary[**location** | **private** | **standby**]

Syntax Description

location	Displays location specific information.
private	Displays private information.
standby	Displays standby node specific information.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.2	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
l2vpn	read

Example

This sample output shows the EVPN summary:

```
RP/0/RSP0/CPU0:router#show evpn summary
Thu Jul  4 01:34:58.838 DST
----------------------------
Global Information
----------------------------
Number of EVIs                : 1
Number of Local MAC Routes    : 1
Number of Remote MAC Routes   : 0
Number of Local IMCAST Routes : 0
Number of Remote IMCAST Routes: 0
Number of Internal Labels     : 0
Number of ES Entries          : 0
BGP Router ID                 : ::
BGP ASN                       : Invalid
PBB BSA MAC address           : f866.f214.abd7
Global peering timer          :     45 seconds
Global recovery timer         :     20 seconds
```

```
Global programming timer      :   1500 microseconds
Global flushagain timer       :     60 seconds
-----------------------------
High Availability Information
-----------------------------
BGP EOD                       : N
Number of Marked MAC Routes   : 0
Number of Swept MAC Routes    : 0
Number of Marked IMCAST Routes: 0
Number of Swept IMCAST Routes : 0
```

Related Commands

Command	Description
evpn, on page 341	Enters EVPN configuration mode.

show evpn evi

To display the EVPN E-VPN ID information, use the **show evpn evi** command in the EXEC mode.

show evpn evi [**bridge-domain** | **detail** | **inclusive-multicast** | **location** | **mac** | **standby** | **vpn-id**]

Syntax Description

bridge-domain	Displays information for a specified bridge-domain..
detail	Displays detailed information.
inclusive-multicast	Displays EVPN Inclusive Multicast information.
location	Displays location specific information.
mac	Displays EVI MAC route associated configuration information.
standby	Displays standby node specific information.
vpn-id	Displays information for a specified E-VPN Identifier.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.2	This command was introduced.
Release 6.1.2	The show command output is enhanced to display the Service Path Preference parameters.
Release 25.1.1	The **show evpn evi mac** command output is enhanced to display the multi-paths internal ID.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN EVI information with the VPN-ID and MAC address filter:

```
RP/0/RSP0/CPU0:router#show evpn evi vpn-id 185 mac 0024.be03.ce01
MAC address    Nexthop                                 Label    vpn-id
-------------- --------------------------------------- -------- --------
0024.be03.ce01 3.100.100.100                           16004    185
               4.100.100.100                           16004    185
   ESI port key : 0x0000
   Source       : Remote
   Flush Count  : 0
```

This sample output shows the EVPN EVI information with the VPN-ID and inclusive-multicast filter:

```
RP/0/RSP0/CPU0:router#show evpn evi vpn-id 185 inclusive-multicast service-id 1850312 orig-ip
 1.100.100.100
ISID          Originating IP                vpn-id
------------- ----------------------------- ----------
1850312       1.100.100.100                           185
1850312       2.100.100.100                           185
1850312       3.100.100.100                           185
1850312       4.100.100.100                           185
```

This sample output shows the EVPN EVI inclusive-multicast information:

```
RP/0/RSP0/CPU0:router#show evpn evi inclusive-multicast detail
ISID: 1850312, Originating IP: 1.100.100.100                              185
    Nexthop: ::
    Label  : 16005
    Source : Local
ISID: 1850312, Originating IP: 2.100.100.100                              185
    Nexthop: 2.100.100.100
    Label  : 16005
    Source : Remote
ISID: 1850312, Originating IP: 3.100.100.100                              185
    Nexthop: 3.100.100.100
    Label  : 16005
    Source : Remote
ISID: 1850312, Originating IP: 4.100.100.100                              185
    Nexthop: 4.100.100.100
    Label  : 16005
    Source : Remote
```

This sample output shows the EVPN EVI information with the bridge-domain filter:

```
RP/0/RSP0/CPU0:router#show evpn evi bridge-domain tb1-core1 detail
EVI        Bridge Domain                Type
---------- ---------------------------- -------
145        tb1-core1                    PBB
165        tb1-core2                    PBB
185        tb1-core3                    PBB
65535      ES:GLOBAL                    BD
```

This sample output shows the EVPN EVI detailed information:

```
RP/0/RSP0/CPU0:router#show evpn evi detail
EVI        Bridge Domain                Type
---------- ---------------------------- -------
145        tb1-core1                    PBB
   Unicast Label  : 16000
   Multicast Label: 16001
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:145
   RT Auto  : 100:145
   Route Targets in Use           Type
   ------------------------------ -------
   100:145                        Import
   100:145                        Export
```

```
165        tb1-core2                    PBB
   Unicast Label  : 16002
   Multicast Label: 16003
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:165
   RT Auto  : 100:165
   Route Targets in Use           Type
   ------------------------------ -------
   100:165                        Import
   100:165                        Export

185        tb1-core3                    PBB
   Unicast Label  : 16004
   Multicast Label: 16005
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:185
   RT Auto  : 100:185
   Route Targets in Use           Type
   ------------------------------ -------
   100:185                        Import
   100:185                        Export

65535      ES:GLOBAL                    BD
   Unicast Label  : 0
   Multicast Label: 0
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:0
   RT Auto  : none
   Route Targets in Use           Type
   ------------------------------ -------
   0100.9e00.0210                 Import
   0100.be01.ce00                 Import
   0100.be02.0101                 Import
```

This sample output shows the EVPN EVI information with the MAC address filter:

```
Router# show evpn evi mac ee04.0700.0450 detail

VPN-ID     Encap      MAC address    IP address                              Nexthop
                           Label    SID
---------- ---------- -------------- ----------------------------------------
---------------------------------------- -------- ----------------------------------------
12         MPLS       ee04.0700.0450 ::                                      192.168.0.4
                           24171
   Ethernet Tag                          : 0
   Multi-paths Resolved                  : True
   Multi-paths Internal label            : 29022
   Service Group ID                      : None
   Local Static                          : No
   Remote Static                         : Yes
   Local Ethernet Segment                : N/A
   Remote Ethernet Segment               : 0001.0001.0001.0701.0007
   Local Sequence Number                 : N/A
   Remote Sequence Number                : 0
   Local Encapsulation                   : N/A
   Remote Encapsulation                  : MPLS
   Local E-Tree                          : Root
   Remote E-Tree                         : Root
   Remote matching E-Tree RT             : No
   Local AC-ID                           : 0x0
   Remote AC-ID                          : 0x45
   Local ARP/ND Information              : N/A
   Remote ARP/ND Information             : N/A
```

From Release 25.1.1, the command output displays multi-paths internal ID. In this example, the multi-paths internal ID shows "none", but for SRv6 MACs, it displays a specific value.

```
Router# show evpn evi mac ee04.0700.0450 detail

VPN-ID     Encap      MAC address    IP address                              Nexthop
                           Label    SID
---------- ---------- -------------- ----------------------------------------
------------------------------------ -------- ----------------------------------------
12         MPLS       ee04.0700.0450 ::                                      192.168.0.4
                           24171
   Ethernet Tag                          : 0
   Multi-paths Resolved                  : True
   Multi-paths Internal label            : 29022
   Multi-paths Internal ID               : None
   Service Group ID                      : None
   Local Static                          : No
   Remote Static                         : Yes
   Local Ethernet Segment                : N/A
   Remote Ethernet Segment               : 0001.0001.0001.0701.0007
   Local Sequence Number                 : N/A
   Remote Sequence Number                : 0
   Local Encapsulation                   : N/A
   Remote Encapsulation                  : MPLS
   Local E-Tree                          : Root
   Remote E-Tree                         : Root
   Remote matching E-Tree RT             : No
   Local AC-ID                           : 0x0
   Remote AC-ID                          : 0x45
   Local ARP/ND Information              : N/A
   Remote ARP/ND Information             : N/A
```

Related Commands

Command	Description
evpn, on page 341	Enters EVPN configuration mode.
evpn evi, on page 342	

show evpn internal-label

To display EVPN internal label associated configuration information, use the **show evpn internal-label** command in the EXEC mode.

show evpn internal-label [**vpn-id** *evi* [**detail**]]

Syntax Description

vpn-id *evi*	Displays information for a specified E-VPN Identifier.
detail	Displays detailed information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.21	This command was introduced.
Release 25.1.1	The command output is enhanced to display the path version.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN internal label associated configuration information.

```
Router# show evpn internal-label vpn-id 15 tag 60 detail

VPN-ID     Encap  Ethernet Segment Id         EtherTag     Label
---------- ------ -------------------------- ----------   --------
15         MPLS   0001.0001.0001.1101.0011    60           28665
   Multi-paths resolved: TRUE (Remote port-active)
   Multi-paths Internal label: 28665
    EAD/ES  (ID:0x00000000000014c0)
            (P) 192.168.0.3                               0
    EAD/EVI (ID:0x00000000000014bf)
            (P) SR-TE BSID 28470
   Summary pathlist (ID 0x00000000000014c2):
 0x02000009 (P) SR-TE BSID 28470
```

From Release 25.1.1, the command output displays path version.

```
Router# show evpn internal-label vpn-id 15 tag 60 detail
```

```
VPN-ID     Encap  Ethernet Segment Id         EtherTag     Label
---------- ------ -------------------------- ----------   --------
15         MPLS   0001.0001.0001.1101.0011    60           28665
   Multi-paths resolved: TRUE (Remote port-active)
   Multi-paths Internal label: 28665
    EAD/ES  (ID:0x00000000000014c0)
            (P) 192.168.0.3                               0
                  Path Version:2, Originating PE:::
    EAD/EVI (ID:0x00000000000014bf)
            (P) SR-TE BSID 28470
   Summary pathlist (ID 0x00000000000014c2):
 0x02000009 (P) SR-TE BSID 28470
```

weight

To configure the weight of a PE that can be used for EVPN Designated Forwarder (DF) election, use the **weight** command in the EVPN interface Ethernet segment service carving configuration mode.

weight *weight-value*

Syntax Description

weight-value	Specifies the preference DF weight. The range is from 0 to 65535 unless access-driven is configured, in which case it will be 0 to 32767. Default is 32767 when not configured.

Command Default

None

Command Modes

EVPN interface Ethernet segment service carving configuration mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows configuration of DF weight.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 01.11.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode port-active
Router(config-evpn-ac-es)# service-carving preference-based
Router(config-evpn-ac-es-sc-pref)# weight 100
Router(config-evpn-ac-es-sc-pref)# commit
```



Layer 2 Access List Commands

For detailed information about Ethernet services ACL concepts, configuration tasks, and examples, see the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*.

- copy access-list ethernet-service, on page 378
- deny (ES ACL), on page 380
- ethernet-service access-group, on page 383
- ethernet-services access-list, on page 385
- permit (ES ACL), on page 387
- resequence access-list ethernet-service, on page 390
- show access-lists ethernet-services, on page 392
- show access-lists ethernet-services trace, on page 396
- show access-list ethernet-service usage pfilter, on page 398
- show lpts pifib hardware entry optimized, on page 400

copy access-list ethernet-service

To create a copy of an existing Ethernet services access list, use the **copy access-list ethernet-services** command in EXEC mode.

copy access-list ethernet-service *source-acl destination-acl*

Syntax Description

source-acl	Name of the access list to be copied.
destination-acl	Name of the destination access list where the contents of the *source-acl* argument is copied.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **copy access-list ethernet-service** command to copy a configured Ethernet services access list. Use the *source-acl* argument to specify the access list to be copied and the *destination-acl* argument to specify where to copy the contents of the source access list. The *destination-acl* argument must be a unique name; if the *destination-acl* argument name already exists for an access list, the access list is not copied. The **copy access-list ethernet-service** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists.

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

In the following example, a copy of access list list-1 is created as list-2:

```
RP/0/RSP0/CPU0:router# show access-list ethernet-service list-1

ethernet service access-list list-1
  10 permit any any
  20 permit 2.3.4 5.4.3
RP/0/RSP0/CPU0:router# copy access-list ethernet-service list-1 list-2
RP/0/RSP0/CPU0:router# show access-list ethernet-service list-2
ethernet service access-list list2
```

```
10 permit any any
20 permit 2.3.4 5.4.3
```

Related Commands

Command	Description
deny (ES ACL), on page 380	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 383	Controls access to an interface.
ethernet-services access-list, on page 385	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 387	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 390	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 392	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 396	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 398	Identifies the modes and interfaces on which a particular ACL is applied.

deny (ES ACL)

To set conditions for an Ethernet services access list, use the **deny** command in Ethernet services access list configuration mode. To remove a condition, use the **no** form of the command.

[*sequence-number*] **deny** {*src-mac-address src-mac-mask* | **any** | **host** | *dest-mac-address dest-mac-mask*} [*ethertype-number* | **capture** | **vlan** *min-vlan-ID* [*max-vlan-ID*]] [**cos** *cos-value*] [**dei**] [**inner-vlan** *min-vlan-ID* [*max-vlan-ID*]] [**inner-cos** *cos-value*] [**inner-dei**]
no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **deny** statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the **resequence access-list ethernet-service** command to change the number of the first statement and increment subsequent statements of a configured access list.
src-mac-address	Source MAC address in format *H.H.H*.
src-mac-mask	Source MAC mask in format *H.H.H*.
any	Denies any source MAC address and mask.
host	Denies host with a specific host source MAC address and mask, in format *H.H.H*.
dest-mac-address	Destination MAC address in format *H.H.H*.
dest-mac-mask	Destination MAC mask in format *H.H.H*.
ethertype-number	16-bit ethertype number in hexadecimal. Range is 0x1 to 0xffff.
capture	(Optional) Captures packets using the traffic mirroring feature and copies this to a capture file.
vlan	(Optional) Denies a specific VLAN or a range of VLANs.
min-vlan-ID	ID for a specific VLAN or the beginning of a range of VLAN IDs.
max-vlan-ID	(Optional) ID for the end of a range of VLAN IDs.
cos	(Optional) Denies based on class of service value.
cos-value	Class of service value. Range is from 0 to 7.
dei	(Optional) Denies based on the setting of the discard eligibility indicator (DEI).
inner-vlan	(Optional) Denies a specific VLAN ID or range of VLAN IDs for the inner header.
min-vlan-ID	ID for a specific VLAN or the beginning of a range of VLAN IDs.
max-vlan-ID	(Optional) ID for the end of a range of VLAN IDs.
inner-cos	(Optional) Denies based on inner header class of service value.

cos-value	Inner header class of service value. Range is from 0 to 7.
inner-dei	(Optional) Denies based on inner header discard eligibility indicator.

Command Default

There is no default condition under which a packet is denied passing the Ethernet services access list.

Command Modes

Ethernet services access list configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **deny** command following the **ethernet-service access-list** command to specify conditions under which a packet can pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit** or **deny** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

If you want to add a statement between two consecutively numbered statements (for example, between lines 10 and 11), first use the resequence access-list ethernet-service, on page 390 command to renumber the first statement and increment the entry number of each subsequent statement.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to define an Ethernet services access list named L2ACL1:

```
RP/0/RSP0/CPU0:router(config)# ethernet-services access-list L2ACL1
RP/0/RSP0/CPU0:router(config-es-acl)# 10 permit 00ff.eedd.0010 ff00.0000.00ff 0011.ab10.cdef
 ffff.0000.ff00 vlan 1000-1100  inner-vlan 100 inner-cos 7 inner-dei
RP/0/RSP0/CPU0:router(config-es-acl)# 20 deny host eedd.0011.ff1c ff00.0000.00ff any vlan
300  cos 1 dei inner-vlan 30 inner-cos 6
RP/0/RSP0/CPU0:router(config-es-acl)# 30 permit any any vlan 500 cos 2 inner-vlan 600
inner-cos 5 inner-dei
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 378	Creates a copy of an existing Ethernet services access list.
ethernet-service access-group, on page 383	Controls access to an interface.

Command	Description
ethernet-services access-list, on page 385	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 387	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 390	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 392	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 396	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 398	Identifies the modes and interfaces on which a particular ACL is applied.

ethernet-service access-group

To control access to an interface, use the **ethernet-service access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of the command.

ethernet-service access-group *access-list-name* {**ingress** | **egress**}
no ethernet-service access-group *access-list-name* {**ingress** | **egress**}

Syntax Description

access-list-name	Name of an Ethernet services access list as specified by the **ethernet-service access-list** command.
ingress	Filters on inbound packets.
egress	Filters on outbound packets.

Command Default

The interface does not have an Ethernet services access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **ethernet-service access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *acl-name* argument to specify a particular Ethernet services access list. Use the **ingress** keyword to filter on inbound packets or the **egress** keyword to filter on outbound packets.

If the list permits the addresses, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns a host unreachable message.

If the specified access list does not exist, all packets are passed.

By default, the unique or per-interface ACL statistics are disabled.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example show how to apply filters on packets inbound and outbound from GigabitEthernet interface 0/2/0/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ethernet-service access-group p-ingress-filter ingress
RP/0/RSP0/CPU0:router(config-if)# ethernet-service access-group p-egress-filter egress
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 378	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 380	Sets conditions for an Ethernet services access list
ethernet-services access-list, on page 385	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 387	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 390	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 392	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 396	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 398	Identifies the modes and interfaces on which a particular ACL is applied.

ethernet-services access-list

To define an Ethernet services (Layer 2) access list by name, use the **ethernet-services access-list** command in global configuration mode. To remove all entries in an Ethernet services access list, use the **no** form of the command.

ethernet-services access-list *access-list-name*
no ethernet-services access-list *access-list-name*

Syntax Description

access-list-name	Name of the Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.

Command Default

No Ethernet services access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **ethernet-services access-list** command places the router in access list configuration mode, in which the denied or permitted access conditions must be defined with the **deny** (ES ACL) or **permit** (ES ACL) command.

Use the resequence access-list ethernet-service, on page 390 command if you need to add a **permit** or **deny** statement between consecutive entries in an existing Ethernet services access lists.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to define an Ethernet services access list named L2ACL1:

```
RP/0/RSP0/CPU0:router(config)# ethernet-services access-list L2ACL1
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 378	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 380	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 383	Controls access to an interface.

Command	Description
permit (ES ACL), on page 387	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 390	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 392	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 396	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 398	Identifies the modes and interfaces on which a particular ACL is applied.

permit (ES ACL)

To set conditions for an Ethernet services access list, use the **permit** command in Ethernet services access list configuration mode. To remove a condition, use the **no** form of the command.

[*sequence-number*] **permit** {*src-mac-address src-mac-mask* | **any** | **host** | *dest-mac-address dest-mac-mask*} [*ethertype-number* | **capture** | **vlan** *min-vlan-ID* [*max-vlan-ID*]] [**cos** *cos-value*] [**dei**] [**inner-vlan** *min-vlan-ID* [*max-vlan-ID*]] [**inner-cos** *cos-value*] [**inner-dei**]
no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the **resequence access-list ethernet-service** command to change the number of the first statement and increment subsequent statements of a configured access list.
src-mac-address	Source MAC address in format *H.H.H*.
src-mac-mac	Source MAC mask in format *H.H.H*.
any	Permits any source MAC address and mask.
host	Permits host with a specific host source MAC address and mask, in format *H.H.H*.
dest-mac-address	Destination MAC address in format *H.H.H*.
dest-mac-mac	Destination MAC mask in format *H.H.H*.
ethertype-number	16-bit ethertype number in hexadecimal. Range is 0x1 to 0xffff.
capture	(Optional) Captures packets using the traffic mirroring feature and copies this to a capture file.
vlan	(Optional) Permits a specific VLAN or a range of VLANs.
min-vlan-ID	ID for a specific VLAN or the beginning of a range of VLAN IDs.
max-vlan-ID	(Optional) ID for the end of a range of VLAN IDs.
cos	(Optional) Permits based on class of service value.
cos-value	Class of service value. Range is from 0 to 7.
dei	(Optional) Permits based on the setting of the discard eligibility indicator (DEI).
inner-vlan	(Optional) Permits a specific VLAN ID or range of VLAN IDs for the inner header.
min-vlan-ID	ID for a specific VLAN or the beginning of a range of VLAN IDs.
max-vlan-ID	(Optional) ID for the end of a range of VLAN IDs.
inner-cos	(Optional) Permits based on inner header class of service value.

cos-value	Inner header class of service value. Range is from 0 to 7.
inner-dei	(Optional) Permits based on inner header discard eligibility indicator.

Command Default

There is no specific default condition under which a packet is permitted passing the Ethernet services ACL.

Command Modes

Ethernet services access list configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **permit** command following the **ethernet-service access-list** command to specify conditions under which a packet can pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit** or **deny** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

If you want to add a statement between two consecutively numbered statements (for example, between lines 10 and 11), first use the resequence access-list ethernet-service, on page 390 command to renumber the first statement and increment the entry number of each subsequent statement.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example show how to set a permit condition for an access list named L2ACL1:

```
RP/0/RSP0/CPU0:router(config)# ethernet-services access-list L2ACL1
RP/0/RSP0/CPU0:router(config-es-al)# 10 permit 00ff.eedd.0010 ff00.0000.00ff 0011.ab10.cdef
 ffff.0000.ff00 vlan 1000-1100  inner-vlan 100 inner-cos 7 inner-dei
RP/0/RSP0/CPU0:router(config-es-al)# 20 permit any host 000a.000b.000c 0800 vlan 500 cos 2
 inner-vlan 600 inner-cos 5 inner-dei
RP/0/RSP0/CPU0:router(config-es-al)# 30 permit any host 000a.000b.000c 8137 vlan 500 cos 2
 inner-vlan 600 inner-cos 5 inner-dei
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 378	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 380	Sets conditions for an Ethernet services access list

Command	Description
ethernet-service access-group, on page 383	Controls access to an interface.
ethernet-services access-list, on page 385	Defines an Ethernet services (Layer 2) access list by name.
resequence access-list ethernet-service, on page 390	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 392	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 396	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 398	Identifies the modes and interfaces on which a particular ACL is applied.

resequence access-list ethernet-service

To renumber existing statements and increment subsequent statements to allow a new Ethernet services access list statement, use the **resequence access-list ethernet-service** command in EXEC mode.

resequence access-list ethernet-service *access-list-name* [*starting-sequence-number* [*increment*]]

Syntax Description

access-list-name	Name of the Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
starting-sequence-number	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. Maximum value is 2147483646. Default is 10.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483646. Default is 10.

Command Default

starting-sequence-number: 10

increment: 10

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **resequence access-list ethernet-service** command to add a permit or deny statement between consecutive entries in an existing Ethernet services access list. Specify the first entry number (the *start-sequence-number*) and the increment by which to separate the entry numbers of the statements. the software remembers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

In the following example, suppose you have an existing access list:

```
ethernet service access-list L2ACL1
  10 permit 1.2.3 4.5.6
```

```
  20 deny 2.3.4 5.4.3
  30 permit 3.1.2 5.3.4 cos 5
```

You need to add additional entries in the access list ahead of the first permit statement. First, you resequence the entries, renumbering the statements starting with number 20 and an increment of 10, and then you have room for additional statements between each of the existing statements:

```
RP/0/RSP0/CPU0:router# resequence access-list ethernet-service L2ACL1 20 10
RP/0/RSP0/CPU0:router# show access-list ethernet-services L2ACL1

ethernet service access-list L2ACL1
  20 permit 1.2.3 4.5.6
  30 deny 2.3.4 5.4.3
  40 permit 3.1.2 5.3.4 cos 5
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 378	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 380	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 383	Controls access to an interface.
ethernet-services access-list, on page 385	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 387	Sets conditions for an Ethernet services access list.
show access-lists ethernet-services, on page 392	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 396	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 398	Identifies the modes and interfaces on which a particular ACL is applied.

show access-lists ethernet-services

To display the contents of current Ethernet services access lists, use the **show access-lists ethernet-services** command in EXEC mode.

show access-lists ethernet-services [*access-list-name* | **maximum** | **standby** | **summary**] [**hardware** | **usage**] [**ingress** | **egress**] [**implicit** | **detail** | **sequence** | **location** *location*]

Syntax Description

access-list-name	(Optional) Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
maximum	(Optional) Show the maximum number of configurable Ethernet services ACLs and ACEs.
standby	(Optional) Display all access lists in standby mode.
summary	(Optional) Display a summary of Ethernet services access lists.
hardware	(Optional) Display Ethernet services access list entries in hardware including the match count for a specific ACL in a particular direction across the line card.
usage	(Optional) Display the usage of this ACL in a given location.
ingress	(Optional) Filters on inbound packets.
egress	(Optional) Filters on outbound packets.
implicit	(Optional) Display the count of packets implicitly denied by a particular ACL.
detail	(Optional) Display TCAM entries.
sequence	(Optional) Display statistics for a specific sequence number.
sequence-number	Sequence number value. Range is 1 to 2147483647.
location	(Optional) Display information for a specific node number.
location	Fully qualified location specification

Command Default

The contents of all Ethernet services access lists are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
acl	read, write

Examples

The following examples lists defined Ethernet services access list maximum thresholds:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services maximum

  Max configurable ACLs: 10000
  Max configurable ACEs: 350000

RP/0/RSP0/CPU0:router# show access-lists ethernet-services maximum detail

  Total ACLs configured: 2
  Total ACEs configured: 3
  Max configurable ACLs: 10000
  Max configurable ACEs: 350000
```

The following example lists the Ethernet services access-list standby:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services standby

ethernet-services access-list i
 10 permit host 0001.0002.0003 host 000a.000b.000c
ethernet-services access-list l2_acl
 10 permit any any
 20 deny host 0002.0003.0004 host 000.50004.0003
```

The following example displays a summary of the number of Ethernet services ACLs configured on the system:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services summary

ACL Summary:
  Total ACLs configured: 2
  Total ACEs configured: 3
```

The following example displays the number of packets matching the access list l2_acl for each ACE:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services l2_ACL hardware ingress location
 0/0/CPU0

ethernet service access-list l2_acl
  10 permit any any ( 3524 hw matches)
  20 deny host 0002.0003.0004 host 0005.0004.0003 (5394 hw matches)
```

The following example displays the number of packets matching the implicit deny in access list l2_acl:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services l2_ACL hardware ingress implicit
 location 0/0/CPU0

ethernet-services access-list l1_acl
 2147483647 implicit deny any any (2300 hw matches)
```

The following example displays the number of packets matching a particular sequence number:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services l2_ACL hardware ingress sequence
 20 location 0/0/CPU0

ethernet-services access-list l2_acl
 20 deny host 0002.0003.0004 host 0005.0004.0003 (5394 hw matches)
```

The following example displays statistics for the TCAM entry for Ethernet services access list l2acl_4:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services l2acl_4 hardware ingress sequence
 10 detail location 0/6/CPU0
Wed Jun 24 00:28:51.367 UTC

ACL name: l2acl_4
Format type : 1
Channel ID: 2
Sequence Number: 10
Grant: permit
Logging: OFF
Hits: 0
Statistics pointer: 0x150628
Number of TCAM entries: 1
idx = 0
Entry : 0 for ACE : 10
RAW value  : 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
RAW mask   : 00 03 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

-------------------------------Field Details----------------------------------
outer_vlan_id value     : 0000
outer_vlan_id mask      : 0ffff
outer_vlan discard eligibility value: 00
outer_vlan discard eligibility mask : 01
outer_vlan_id cos value: 00
outer_vlan_id cos mask: 07
Ethernet type value     : 0000
Ethernet type mask      : ffff
Base app id value     : 02
Base app id value     : 00
Base acl id value    : 0001
Base acl id mask     : 0000
outer vlan id present value     : 0
outer vlan id present mask      : 1
inner vlan id present value     : 0
inner vlan id present mask      : 1
Mac source address value     : 0000 0000 0000
Mac source address mask      : ffff ffff ffff
Mac destination address value  : 0000 0000 0000
Mac destination address mask   : ffff ffff ffff
RP/0/RSP0/CPU0:router#
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 378	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 380	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 383	Controls access to an interface.
ethernet-services access-list, on page 385	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 387	Sets conditions for an Ethernet services access list.

Command	Description
resequence access-list ethernet-service, on page 390	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services trace, on page 396	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 398	Identifies the modes and interfaces on which a particular ACL is applied.

show access-lists ethernet-services trace

To display Ethernet services access list trace information use the **show access-lists ethernet-services trace** command in EXEC mode.

show access-lists ethernet-services trace {**client** | **intermittent** | **critical** | **both** | **all**}

Syntax Description

client	Trace data for ES ACL client.
intermittent	Trace data for intermittent failures.
critical	Trace data for server-critical failures
both	Trace data for server-critical and intermittent failures.
all	Trace data for server-critical and intermittent failures.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
acl	read

Examples

The following examples show how to display Ethernet services access list trace information:

```
RP/0/RSP0/CPU0:router# show access-lists ethernet-services trace all
1 unique entries (256 possible, 0 filtered)
Jun 15 06:42:56.980 es/acl_mgr_un 0/RSP0/CPU0 1#t3 Manager state is active
3 wrapping entries (1024 possible, 0 filtered, 3 total)
Jun 15 06:42:57.053 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:23:30.075 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:29:41.383 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 2 batches

RP/0/RSP0/CPU0:router# show access-lists ethernet-services trace both
1 unique entries (256 possible, 0 filtered)
Jun 15 06:42:56.980 es/acl_mgr_un 0/RSP0/CPU0 1#t3 Manager state is active
3 wrapping entries (1024 possible, 0 filtered, 3 total)
Jun 15 06:42:57.053 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
```

```
 1 batches
Jun 16 02:23:30.075 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:29:41.383 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 2 batches

RP/0/RSP0/CPU0:router# show access-lists ethernet-services trace critical
1 unique entries (256 possible, 0 filtered)
Jun 15 06:42:56.980 es/acl_mgr_un 0/RSP0/CPU0 1#t3 Manager state is active

RP/0/RSP0/CPU0:router# show access-lists ethernet-services trace intermittent
3 wrapping entries (1024 possible, 0 filtered, 3 total)
Jun 15 06:42:57.053 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:23:30.075 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 1 batches
Jun 16 02:29:41.383 es/acl_mgr/es_acl_mgr_wr 0/RSP0/CPU0t1 es_aclmgr_verify acl_add: verifying
 2 batches
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 378	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 380	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 383	Controls access to an interface.
ethernet-services access-list, on page 385	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 387	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 390	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 392	Displays the contents of current Ethernet services access lists.
show access-list ethernet-service usage pfilter, on page 398	Identifies the modes and interfaces on which a particular ACL is applied.

show access-list ethernet-service usage pfilter

To identify the modes and interfaces on which a particular ACL is applied, use the **show access-list ethernet-service usage pfilter** command in EXEC mode. Information displayed includes the application of all or specific ACLs, the interfaces on which they have been applied and the direction in which they are applied.

show access-list ethernet-services [*access-list-name*] **usage pfilter location** {*location* | **all**}

Syntax Description

access-list-name	(Optional) Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
location	Interface card on which the access list information is needed.
location	Fully qualified location specification.
all	Displays packet filtering usage for all interface cards.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to display packet filter usage at a specific location:

```
RP/0/RSP0/CPU0:router# show access-list ethernet-services usage pfilter location 0/0/cpu0
pfilter location 0/0/cpu0
Interface : GigabitEthernet0/0/0/9
    Input ACL : l2_acl
    Output ACL : N/A
Interface : GigabitEthernet0/0/0/30
    Input ACL : N/A
    Output ACL : i
```

The following example shows the results of the command for a specific ACL:

```
RP/0/RSP0/CPU0:router# show access-list ethernet-services l2_acl usage pfilter location
```

```
0/0/CPU0
Interface : GigabitEthernet0/0/0/9
    Input ACL : l2_acl
    Output ACL : N/A
```

Related Commands

Command	Description
copy access-list ethernet-service, on page 378	Creates a copy of an existing Ethernet services access list.
deny (ES ACL), on page 380	Sets conditions for an Ethernet services access list
ethernet-service access-group, on page 383	Controls access to an interface.
ethernet-services access-list, on page 385	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 387	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 390	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 392	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 396	Displays Ethernet services access list trace information.

show lpts pifib hardware entry optimized

To display a set of optimized entries that are combined as a single entry, inside the Ternary Content Addressable Memory (TCAM), use the **show lpts pifib hardware entry optimized** command in EXEC mode.

show lpts pifib hardware entry optimized *location*

Syntax Description

location	Mandatory. The location of the line card where the interface is present.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
lpts	read

The following example shows the output of the **show lpts pifib hardware entry optimized**command:

```
RP/0/RSP0/CPU0:router# show lpts pifib hardware entry optimized location 0/4/CPU0
Node: 0/4/CPU0:
----------------------------------------
Protocol - Layer4 Protocol; Intf - Interface in optimized list

Protocol   laddr.Port, raddr.Port    Intf            VRF id       State
---------- ------------------------- --------------- ------------ --------------------
IGMP       224.0.0.22.any , any.any  Te0/4/0/0       *            Uidb Set
                                     Te0/4/0/1       *            Uidb Set

           224.0.0.22.any , any.any  Te0/4/0/0       *            Uidb Set
                                     Te0/4/0/1       *            Uidb Set

           any.any , any.any         Te0/4/0/0       *            Uidb Set
                                     Te0/4/0/1       *            Uidb Set
```



VXLAN Commands

For detailed information about VXLAN concepts, configuration tasks, and examples, see the *L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers*.

- anycast source-interface loopback, on page 402
- interface nve, on page 403
- member, on page 404
- member vni, on page 406
- overlay-encapsulation, on page 407
- show nve interface, on page 408
- show nve peers, on page 409
- show nve vni, on page 410
- source-interface loopback, on page 411

anycast source-interface loopback

To configure the anycast mode parameters for the VXLAN Tunnel EndPoint (VTEP), use the **anycast source-interface loopback** command in interface configuration submode.

anycast source-interface loopback *loopback-interface-identifier* **sync-group** *ip-address*

Syntax Description

anycast	Configures the anycast mode parameters for the VTEP.
source-interface loopback *loopback-interface-identifier*	Configures loopback interface as the source interface for the VTEP. The variable *loopback-interface-identifier* is the loopback interface instance.
sync-group *ip-address*	Assigns a bidirectional multicast group for synchronization between anycast gateways.

Command Default

None

Command Modes

Interface configuration submode

Command History

Release	Modification
Release 5.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

This example shows how to configure anycast mode parameters for VTEP.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface nve 45
RP/0/RSP0/CPU0:router(config-if)# overlay-encapsulation vxlan
RP/0/RSP0/CPU0:router(config-if)# source-interface loopback 0
RP/0/RSP0/CPU0:router(config-if)# member vni 1 mcast-group 192.20.9.2 0.0.0.0
RP/0/RSP0/CPU0:router(config-if)# anycast source-interface loopback 0 sync-group 192.20.9.2
```

interface nve

To create a network virtualization endpoint (NVE) interface and enter the NVE interface configuration mode, use the **interface nve** command in Global Configuration mode. To remove the NVE interface, use the **no** form of this command.

interface nve *nve-id*

Syntax Description

nve-id	The NVE interface ID. It can take values from 1 to 65535.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
interface	read, write

Example

The following example shows how to create an NVE interface and enter the NVE interface configuration mode.

```
RP/0/RSP0/CPU0:router(config)# interface nve 1
RP/0/RSP0/CPU0:router(config-if)#
```

member

To associate a VNI member or range of members with the NVE interface and set the multicast group, use the **member** command in NVE interface configuration mode. To disassociate the VNI member or range, use the **no** form of this command.

member vni {*numberstart_number-end_number*} **mcast-group** *ip_address* [*end_ip_address*]

Syntax Description

vni	The member VNI.
number	The VNI for a single VXLAN. The valid values are from 1 to 16777215.
start_number	The first VNI from a range.
end_number	The end VNI from a range.
mcast-group	The multicast group.
ip_address	A single multicast IP address or the starting multicast IP address from a range.
end_ip_address	The end multicast IP address from a range.

Command Default

None

Command Modes

NVE interface configuration

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step for each VXLAN or VXLAN range. For instance,

```
RP/0/RSP0/CPU0:router(config-if)# member vni 10 mcast-group 224.2.2.10
RP/0/RSP0/CPU0:router(config-if)# member vni 23 mcast-group 224.2.2.23
RP/0/RSP0/CPU0:router(config-if)# member vni 50-59 mcast-group 224.2.2.50 224.2.2.59
RP/0/RSP0/CPU0:router(config-if)# member vni 100-120 mcast-group 224.2.2.100 224.2.2.120
```

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
interface	read, write
tunnel	read, write

Example

The following example shows VNIs from 5000 to 5009 associated with the nve interface "1" and multicast IP address range 200.0.0.1 to 200.0.0.20.

```
RP/0/RSP0/CPU0:router(config)# interface nve 1
RP/0/RSP0/CPU0:router(config-if)# overlay-encapsulation vxlan
RP/0/RSP0/CPU0:router(config-if)# member vni 5000-5009 mcast-group 228.0.0.0 228.0.0.9
```

member vni

To map a VXLAN to a bridge domain, use the **member vni** command in bridge-domain configuration mode. To remove the VXLAN from the bridge domain, use the **no** form of this command.

member vni *number*

Syntax Description

vni	The member virtual network identifier (VNI).
number	The ID of the VXLAN to be mapped to the bridge domain. The valid values are from 1 to 16777215.

Command Default

None

Command Modes

Bridge-domain configuration

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
interface	read, write
tunnel	read, write

Example

The following example shows the VXLAN with VNI "5010" associated with the bridge domain "bd1".

```
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group bg1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain bd1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# member vni 5010
```

overlay-encapsulation

To set a Network Virtualization Endpoint (NVE) interface to provide VXLAN, use the **overlay-encapsulation** command in NVE interface configuration mode. To remove the configured encapsulation on the NVE interface, use the **no** form of this command.

overlay-encapsulation {**vxlan**}

Syntax Description

vxlan	Sets the NVE interface as a VXLAN Terminal EndPoint (VTEP).

Command Default

The NVE interface provides VXLAN encapsulation.

Command Modes

NVE interface configuration

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
interface	read, write
tunnel	read, write

Example

The following example shows an NVE interface configured for VXLAN encapsulation.

```
RP/0/RSP0/CPU0:router(config)# interface nve 1
RP/0/RSP0/CPU0:router(config-if)# overlay-encapsulation vxlan
```

show nve interface

To display the network virtualization endpoint (NVE) interface information, use the **show nve interface** command in EXEC mode.

show nve interface [**detail** | **nve** *nve-id*]

Syntax Description

detail	Displays detailed information about NVE interfaces.
nve *nve-id*	Displays information only about the specified NVE interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
interface	read

Example

The following shows an example output of the **show interface nve** command.

```
RP/0/RSP0/CPU0:router(config)# show interface nve nve1 detail
Interface: nve1, State:up, encapsulation:VXLAN
source-interface: Lo1 (primary:10.0.0.1, secondary:1.1.1.2)

VNI          mcast       VNI state
10.10        239.1.1.1   UP
11.10        239.1.1.1   UP
```

show nve peers

To display the network virtualization endpoint (NVE) peers configured on the router, use the **show nve peers** command in EXEC mode.

show nve peers [**interface nve** *nve-id* | **vni** *vni-id*]

Syntax Description

interface nve *nve-id*	Displays NVE peers of the specified NVE interface.
vni *vni-id*	Displays NVE peers of the specified VNIs.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

The router learns about NVE peers through data plane traffic. Therefore, the **show nve peers** command output displays NVE peers only after VXLAN traffic traverses through the router.

To use this command, you must be in a user group associated with a task 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
tunnel	read

Example

The following shows an example output of the **show nve peers** command.

```
RP/0/RSP0/CPU0:router# show nve peers
Interface  Peer-IP         VNI      Up Time
nve1       10.0.0.1        1000    10h
nve2       10.0.0.2        2000    20h
```

show nve vni

To display list of all VNIs that are associated with various NVE interfaces and the associated multicast IP address that is used for multi-destination frames, use the **show nve vni** command in EXEC mode.

show nve vni [**vni_number** | **detail** | **interface nve** *nve-id*]

Syntax Description

vni_number	Displays output for the specific VXLAN.
detail	Displays more detailed output.
interface nve *nve-id*	Displays details for the specific NVE interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
tunnel	read

Example

The following shows an example output of this show command:

```
RP/0/RSP0/CPU0:router# show nve vni
Interface  VNI          mcast       VNI state
nve1       10.10        239.1.1.1   UP
nve2       11.10        239.1.1.1   UP
```

source-interface loopback

To specify the IP address for a Network Virtualization Endpoint (NVE) interface, use the **source-interface loopback** command to specify a loopback interface whose IP address should be set as the IP address for the NVE interface.

source-interface loopback *interface-id*

Syntax Description

loopback	Specifies a loopback interface as providing IP address for the NVE interface.
interface-id	Specifies the loopback interface ID. It can take values from 0 to 65535.

Command Default

None

Command Modes

NVE interface configuration

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
tunnel	read, write
interface	read, write

Example

The following example shows how to configure the IP address of an NVE interface as the IP address of a loopback interface.

```
RP/0/RSP0/CPU0:router(config)# interface nve 1
RP/0/RSP0/CPU0:router(config-if)# source-interface loopback 1
```