cisco.



VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers, IOS XR Release 6.4.x

Americas Headquarters

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

© 2018 Cisco Systems, Inc. All rights reserved.

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

Cisco Bug Search Tool

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

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE	Preface xvii				
	Changes to This Document xvii				
	Communications, Services, and Additional Information xvii				
CHAPTER 1	Ethernet Interfaces Commands 1				
	dot1q tunneling ethertype 1				
	encapsulation default 3				
	encapsulation dot1ad dot1q 4				
	encapsulation dot1q 5				
	encapsulation dot1q second-dot1q 6				
	encapsulation untagged 8				
	ethernet egress-filter 9				
	ethernet filtering 10				
	ethernet source bypass egress-filter 13				
	l2protocol (Ethernet) 14				
	12transport (Ethernet) 15				
	local-traffic default encapsulation 17				
	rewrite ingress tag 18				
CHAPTER 2	Generic Routing Encapsulation Commands 21				
	bandwidth 21				
	description (GRE) 22				
	ipv4 address 23				
	ipv4 mtu (LxVPN) 24				
	ipv6 address (LxVPN) 25				
	ipv6 mtu (LxVPN) 26				

keepalive 27 mtu (GRE) 28 shutdown (GRE) 28 tunnel destination 29 tunnel key 30 tunnel key-ignore 32 tunnel dfbit 33 tunnel mode 34 tunnel source 35 tunnel tos 36 tunnel ttl 37 tunnel vrf 39

CHAPTER 3

Point to Point Layer 2 Services Commands 41

advertise-mac 43 address-family l2vpn mspw 43 bgp 44 backup (L2VPN) 45 backup disable (L2VPN) 46 clear l2vpn collaborators 47 clear l2vpn counters bridge mac-withdrawal 48 clear l2vpn forwarding counters 49 clear l2vpn forwarding counters bridge-domain mirp-lite 50 clear l2vpn forwarding message counters 51 clear l2vpn forwarding table 52 control-word 52 dynamic-arp-inspection 53 flood mode 55 generic-interface-list 56 global-id (L2VPN) 57 interface (p2p) 58 interworking ipv4 59 ipv4 source 60 12tp static 61

ip-source-guard 63 12transport 64 l2transport l2protocol 66 l2transport propagate 67 l2transport service-policy 68 12vpn 69 load-balancing flow 70 load-balancing pw-label **71** logging (l2vpn) 72 logging nsr 73 monitor-session (l2vpn) 74 mpls static label (L2VPN) 75 neighbor (L2VPN) 76 neighbor evpn 79 neighbor routed 79 nsr (L2VPN) 80 pw-routing 81 preferred-path 82 protocol l2tpv3 83 pw-class (L2VPN) 84 pw-class encapsulation l2tpv3 85 pw-class encapsulation mpls 87 pw-ether 89 pw-grouping 91 p2p 92 rd (L2VPN) 93 sequencing (L2VPN) 94 show bgp l2vpn evpn 95 show bgp l2vpn mspw 97 show bgp vrf-db 98 show evpn evi ead 99 show evpn internal-label 100 show dci-fabric-interconnect 101 show generic-interface-list 103

show l2tp session 105 show l2tp tunnel 106 show l2vpn 108 show l2vpn atom-db 110 show l2vpn collaborators 112 show l2vpn database 113 show l2vpn discovery 115 show l2vpn forwarding **117** show l2vpn forwarding message counters 130 show l2vpn generic-interface-list 132 show l2vpn index 133 show l2vpn nsr 135 show l2vpn process fsm 136 show l2vpn provision queue 138 show l2vpn pw-class 139 show l2vpn pwhe 141 show l2vpn resource 142 show l2vpn trace 143 show l2vpn xconnect 145 show tech-support l2vpn platform no-statistics 157 source (p2p) 158 storm-control 159 tag-impose 161 tos (l2vpn) 162 transport mode (L2VPN) 164 transport mode vlan passthrough 165 ttl (l2vpn) 166 xconnect group 167

CHAPTER 4

Multipoint Layer 2 Services Commands 169

action (VPLS) 170 aging (VPLS) 172 aps-channel 173 autodiscovery bgp 175 bridge-domain (VPLS) 176 bridge group (VPLS) 177 clear l2vpn bridge-domain (VPLS) 178 debug l2vpn forwarding platform vpls all location 179 description (G.8032) 179 dhcp ipv4 snoop profile (VPLS) 180 ethernet ring g8032 181 ethernet ring g8032 profile 182 exclusion list 184 flooding disable 185 flooding unknown-unicast disable (VPLS) 186 igmp snooping disable 187 inclusion-list 188 instance (G.8032) 189 interface (VPLS) 190 12vpn resynchronize forwarding mac-address-table location 191 learning disable (VPLS) 192 level 193 limit (VPLS) 194 mac (VPLS) 196 mac secure 197 maximum (VPLS) 198 monitor interface (port0) 200 monitor interface (port1) 201 mpls static label (VPLS) 202 mtu (VPLS) 203 multicast p2mp 204 neighbor (VPLS) 206 notification (VPLS) 207 open ring 208 port0 interface 209 port1 210 port-down flush disable (VPLS) 211 profile 213

pw-class 214 pw-oam 215 route-target 216 routed 218 rpl 219 show ethernet ring g8032 220 show l2vpn bridge-domain (VPLS) 223 show l2vpn ethernet ring g8032 245 show l2vpn forwarding bridge-domain (VPLS) 247 show l2vpn forwarding bridge-domain mac-address (VPLS) 253 show l2vpn forwarding ethernet ring g8032 258 show l2vpn forwarding protection main-interface 260 show l2vpn protection main-interface 261 shutdown (Bridge Domain) 264 shutdown (VFI) 265 signaling-protocol 266 split-horizon group 267 static-address (VPLS) 268 static-mac-address (VPLS) 269 tcn-propagation 271 time (VPLS) 271 transport rsvp-te 273 type (VPLS) 274 vfi (VPLS) 275 withdraw (VPLS) 276

CHAPTER 5

backbone-source-mac 280 bgp (EVPN) 281 clear mmrp-flood-optimization statistics 283 clear 12vpn forwarding counters bridge-domain mmrp location 283 debug mmrp-flood-optimization packets 284 debug mmrp-flood-optimization protocol 285 ethernet-segment 286

Provider Backbone Bridge Commands 279

ethernet-segment (evpn) 287 evi 288 evpn 289 evpn evi 290 flushagain 291 flood-time 292 force single-homed 293 identifier 294 join-time (PBB) 295 interface (EVPN) 296 leaveall-time (PBB) 297 leave-time (PBB) 298 load-balancing-mode 299 mmrp-flood-optimization 300 mac-flush mvrp 301 mode singleton 302 pbb 303 peering 304 periodic transmit (PBB) 305 programming 306 recovery 307 rewrite ingress tag push 309 service-carving 310 show evpn ethernet-segment 311 show evpn evi 314 show evpn summary 317 show l2vpn bridge-domain pbb 318 show l2vpn forwarding bridge pbb 325 show l2vpn forwarding pbb backbone-source-mac 327 show l2vpn pbb backbone-source-mac 328 show mmrp-flood-optimization 328 static-mac-address 330 timers 332 unknown-unicast-bmac 333

CHAPTER 6

Multiple Spanning Tree Protocol Commands 335

bridge-id 337 bringup delay 339 clear ethernet myrp statistics 340 cost 341 debug ethernet mvrp packets 343 debug ethernet mvrp protocol 344 debug spanning-tree mst packet 345 debug spanning-tree mst protocol-state 347 debug spanning-tree mstag packet 348 debug spanning-tree packet raw 349 debug spanning-tree pvrst 351 debug spanning-tree pvrstag packet 352 debug spanning-tree pvstag packet 354 debug spanning-tree repag packet 355 edge-mode 356 external-cost (MSTAG/REPAG) 357 external-cost (MSTP) 358 flush containment disable 359 forward-delay 360 forward-delay (PVRST) 361 guard root 362 guard topology-change 363 hello-time (Access Gateway) 364 hello-time (MSTP) 366 instance (MSTAG/REPAG) 367 instance (MSTP) 368 instance cost 369 instance port-priority 370 interface (MSTAG/REPAG) 371 interface (MSTP) 373 interface (PVRST) 374 interface (PVSTAG/PVRSTAG) 375

interface (MSTAG Uplink Tracking) 376 join-time 378 leave-time 379 leaveall-time 380 link-type 381 max age 382 maximum (PVRST) 384 maximum age 385 maximum hops (MSTP) 386 mvrp static 387 name (MSTAG/REPAG) 388 name (MSTP) 389 periodic transmit 390 port-id 391 port-priority 393 portfast 395 preempt delay 396 priority (Access Gateway) 397 priority (MSTP) 398 provider-bridge (MSTAG/REPAG) 399 provider-bridge (MSTP) 400 revision (MSTAG/REPAG) 401 revision (MSTP) 402 root-cost 403 root-id 405 root-priority 407 show ethernet mvrp mad 409 show ethernet mvrp statistics 410 show ethernet mvrp status 411 show l2vpn mstp port **412** show l2vpn mstp vlan 414 show spanning-tree mst 415 show spanning-tree mst bpdu interface 417 419 show spanning-tree mst configuration

show spanning-tree mst errors 420 show spanning-tree mst interface 421 show spanning-tree mst topology-change flushes 424 show spanning-tree mstag 426 show spanning-tree mstag bpdu interface 428 show spanning-tree mstag topology-change flushes 429 show spanning-tree mstag tracked **431** show spanning-tree pvrst 432 show spanning-tree pvrstag 435 show spanning-tree pvstag 436 show spanning-tree repag 438 show spanning-tree repag bpdu interface 439 show spanning-tree repag topology-change flushes 441 spanning-tree mst 443 spanning-tree mstag 444 spanning-tree pvrst 445 spanning-tree pvrstag 446 spanning-tree pvstag 447 spanning-tree repag 448 track 449 transmit (PVRST) 450 transmit hold-count 451 vlan 452 vlan (PVRST) 453 vlan-ids (MSTAG/REPAG) 454 vlan-id (MSTP) 455

CHAPTER 7

Layer 2 Access List Commands 457

copy access-list ethernet-service deny (ES ACL) ethernet-service access-group ethernet-services access-list permit (ES ACL) resequence access-list ethernet-service show access-lists ethernet-services 468 show access-lists ethernet-services trace 471 show access-list ethernet-service usage pfilter 473 show lpts pifib hardware entry optimized 474

CHAPTER 8

VXLAN Commands 477

anycast source-interface loopback 477 interface nve 478 member 479 member vni 480 overlay-encapsulation 481 show nve interface 482 show nve peers 483 show nve vni 484 source-interface loopback 484

Contents

I



Preface

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

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

Changes to This Document



This software release has reached end-of-life status. For more information, see the End-of-Life and End-of-Sale Notices.

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

Date	Change Summary
March 2018	Initial release of this document.

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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



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 1
- encapsulation default, on page 3
- encapsulation dot1ad dot1q, on page 4
- encapsulation dot1q, on page 5
- encapsulation dot1q second-dot1q, on page 6
- encapsulation untagged, on page 8
- ethernet egress-filter, on page 9
- ethernet filtering, on page 10
- ethernet source bypass egress-filter, on page 13
- l2protocol (Ethernet), on page 14
- l2transport (Ethernet), on page 15
- local-traffic default encapsulation, on page 17
- rewrite ingress tag, on page 18

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 1	the Ethertype value to 0x92	200.
Command Default	The Ethertype	e field used by peer device	s 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.		
	interface, it c	e 11	hand can be applied to a main interface. When applied to the main that have been configured with an encapsulation dot1q second-dot1q
	This commar	nd changes the outer VLA	N tag from 802.1q Ethertype 0x8100 to 0x9100 or 0x9200.
Task ID	Task Opera ID	ations	
	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
	encapsulatio	on dot1q, on page 5	Defines the matching criteria to map 802.10 frames ingress on an interface to the appropriate service instance.
	encapsulatio 4	on dot1ad dot1q, on page	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.

I

Command	Description
encapsulation dot1q second-dot1q, on page 6	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation untagged, on page 8	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.

	encapsulatio no encapsul	n default ation default		
Syntax Description	This command has no keywords or arguments.			
Command Default	No default se	rvice instance is configured	d on the port.	
Command Modes	Interface con	Interface configuration		
Command History	and History Release Modification			
	Release 3.7.2	2 This command was introduced.		
Usage GuidelinesTo use this command, you must be in a user group associated with a task group that includes a IDs. If the user group assignment is preventing you from using a command, contact your AAA for assistance.If the default service instance is the only one configured on a port, the encapsulation default matches all ingress frames on that port. If the default service instance is configured on a port non-default service instances, the encapsulation default command matches frames that are u those non-default service instances (anything that does not meet the criteria of other services in same physical interface falls into this service instance).				
		If the default service instance is configured on a port that has other sulation default command matches frames that are unmatched by thing that does not meet the criteria of other services instances on the		
			In be configured per interface. If you attempt to configure more than e, 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:		onfigure a service instance on a port:	
	<pre>RP/0/RSP0/CPU0:router(config-if)# encapsulation default</pre>		encapsulation default	
Related Commands	Command		Description	
	encapsulatio	on dot1q, on page 5	Defines the matching criteria to map 802.10 frames ingress on an interface to the appropriate service instance.	

Command	Description
encapsulation dot1ad dot1q, on page 4	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 6	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation untagged, on page 8	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 3	Configure the default service instance on a port.
	encapsulation dot1q, on page 5	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
	encapsulation untagged, on page 8	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 configurati	iguration	
Command History	Release Modi	fication	
	Release 3.7.2 This	command was introduced.	
	Release 3.9.1 The	ingress source-mac keyword was added.	

	Release Modification			
	Release 4.0.1 This command was supported on l2transport subinterfaces.			
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.			
	Only one encapsulation statement can be applied to a subinterface. Encapsulation statements cannot be applied to main interfaces.			
	A single encapsulation dot1q statement specifies matching for frames with a single VLAN ID; a range of VLAN IDs; or a single VLAN ID or untagged.			
Examples	The following example shows how to map 802.1Q frames ingress on an interface to the appropriate service instance:			
	RP/0/RSP0/CPU0:router(config-if	<pre>E) # encapsulation dot1q 10</pre>		
Related Commands	Command	Description		
	encapsulation default, on page 3	Configure the default service instance on a port.		
	encapsulation dot1ad dot1q, on page	e 4 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, page 6	on Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.		
	encapsulation untagged, on page 8	Defines the matching criteria to map untagged ingress Ethernet		

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.

frames on an interface to the appropriate service instance.

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}]}

I

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	e 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:		
	<pre>RP/0/RSP0/CPU0:router(config-if)#</pre>	encapsulation dotlq second-dotlq 20	
Related Commands	Command	Description	
	encapsulation default, on page 3	Configure the default service instance on a port.	
	encapsulation dot1ad dot1q, on page 4	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.	

Command	Description
encapsulation dot1q, on page 5	Defines the matching criteria to map 802.10 frames ingress on an interface to the appropriate service instance.
encapsulation untagged, on page 8	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 crit	teria are defined.	
Command Modes	Interface configu	ration	
Command History	Release N	Iodification	
	Release 3.7.2 T	his command was introduced.	
	Release 3.9.1 T	The ingress source-mac keyword was added.	
Usage Guidelines		nand, you must be in a user group associated w roup assignment is preventing you from using	
	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).		
	protocol traffic,	binterface has a higher priority than the main passes through this subinterface rather than the ied to a main interface having an untagged subi	e main interface. If the ethernet filtering

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 3	Configure the default service instance on a port.
	encapsulation dot1q, on page 5	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
	encapsulation dot1q second-dot1q, on page 6	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. For platforms that support this command, the global default is that subinterface egress encapsulation filtering **Command Default** is disabled. Global configuration and Layer 2 subinterface configuration **Command Modes 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	dotlad Filters only the Ethernet multicast protocol addresses that are reserved by IEEE 802.1ad, use C-facing interfaces, to prevent C-network traffic from interfering with the S-network protocol		1
	dot1q Filters	all Ethernet multicast pro	otocol addresses.
Command Default	Ethernet filtering is not enabled.		
Command Modes	interface confi	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.		

DA MAC Address	Description	dot1q	dot1ad
01-80-C2-00-00-00	STP, RSTP, MSTP, etc.		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
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	CDP, DTP, VTP, PaGP, UDLD	Discard	Data

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

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 dot1g
RP/0/RSP0/CPU0:router(config-if) #12transport
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 dotlg
12transport
 1
L.
interface GigabitEthernet0/5/0/2
shutdown
1
interface GigabitEthernet0/5/0/3
shutdown
!
interface GigabitEthernet0/5/0/4
shutdown
!
interface GigabitEthernet0/5/0/5
shutdown
L.
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 dotlq
1
interface GigabitEthernet0/5/0/1.1 l2transport
encapsulation untagged
1
interface GigabitEthernet0/5/0/2
shutdown
1
interface GigabitEthernet0/5/0/3
shutdown
1
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 Operations ID
	interface read, write
Examples	The following example shows how to mark all ingress packets received on the interface:
	<pre>RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet0/0/0/0/3.1 l2transport RP/0/RSP0/CPU0:router(config-subif)# encapsulation dotlq 1</pre>

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 5	Defines the matching criteria to map 802.10 frames ingress on an interface to the appropriate service instance.

I2protocol (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	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 pro	otocol data units are forwarded through the network without modification.		
Command Modes	Layer 2 transport configuration			
Command History Release Modification		Modification		
	Release 3.9.1	This command was introduced.		
Usage Guidelines		nmand, you must be in a user group associated with a task group that includes appropriate task r group assignment is preventing you from using a command, contact your AAA administrato		

 		
No	te The l2protocol command is avait the l2transport command.	lable only when Layer 2 transport port mode is enabled on the interface with
Task ID	Task Operations ID	
	l2vpn read, write	
Examples	The following example shows how	w to configure an Ethernet interface to tunnel in the ingress direction:
	RP/0/RSP0/CPU0:router(confid	g)# interface TenGigE 0/0/0/1
Related Command	s Command	Description
	l2transport (Ethernet), on page 1	5 Enables Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode.

I2transport (Ethernet)

To enable Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode, use the **l2transport** command in interface 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)# 12transport
RP/0/RSP0/CPU0:router(config-if-l2)# ?
  commit
                 Commit the configuration changes to running
  describe
                 Describe a command without taking real actions
                 Run an exec command
  do
  exit
                 Exit from this submode
                 Negate a command or set its defaults
  no
  service-policy Configure QoS Service policy
                 Show contents of configuration
  show
RP/0/RSP0/CPU0:router(config-if-l2)#
```



Note

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

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)# 12transport
RP/0/RSP0/CPU0:router(config-if-12)#
```

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 dotlq 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 | dot1q vlan-id | 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 Operations ID		
	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 dotlq 10-100 RP/0/RSP0/CPU0:router(config-subif)# local-traffic default encapsulation dotlq 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:		
	<pre>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</pre>		

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 | dot1ad vlan-id | l-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | l-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id | l-to-2 {dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id | l-to-2 {dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id | l-to-2 {dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id | l-to-2 {dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id | l-to-2 {dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id | l-to-2 {dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id | l-to-2 {dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id | dot1ad vlan-id | l-to-2 {dot1q vlan-id | dot1ad vlan-id | dot1ad

Syntax Description	vlan-id	VLAN ID, integer in the range 1 to 4094.			
	push dot1q vlan-id	Pushes one 802.1Q tag with <i>vlan-id</i> .			
	push dot1q <i>vlan-id</i> second-dot1q <i>vlan-id</i>	Pushes a pair of 802.1Q tags in the order first, second.			
	pop {1 2}	One or two tags are removed from the packet. This command can be combined with a push (pop N and subsequent push <i>vlan-id</i>).			
	translate 1-to-1 dot1q vlan-id	Replaces the incoming tag (defined in the encapsulation command) into a different 802.1Q tag at the ingress service instance.			
	translate 2-to-1 dot1q vlan-id	Replaces a pair of tags defined in the 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 int	roduced.			
Usage Guidelines	To use this command, you must be in a user group associated with a task 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 3	Configure the default service instance on a port.	
	encapsulation dot1ad dot1q, on page 4	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 5	Defines the matching criteria to map 802.10 frames ingress on an interface to the appropriate service instance.	
	encapsulation dot1q second-dot1q, on page 6	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.	
	encapsulation untagged, on page 8	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 21
- description (GRE), on page 22
- ipv4 address, on page 23
- ipv4 mtu (LxVPN), on page 24
- ipv6 address (LxVPN), on page 25
- ipv6 mtu (LxVPN), on page 26
- keepalive, on page 27
- mtu (GRE), on page 28
- shutdown (GRE), on page 28
- tunnel destination, on page 29
- tunnel key, on page 30
- tunnel key-ignore, on page 32
- tunnel dfbit, on page 33
- tunnel mode, on page 34
- tunnel source, on page 35
- tunnel tos, on page 36
- tunnel ttl, on page 37
- tunnel vrf, on page 39

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

I

Command Default	None		
Command Modes	interface of	configuration	
Command History	Release	Modification	
	Release 4.2.0	This command was introduced.	
Usage Guidelines		user group assignment is pr	user group associated with a task group that includes appropriate task eventing you from using a command, contact your AAA administrator
Task ID	Task (ID	Operation	
	interface 1	read, write	
	This exam	ple shows how to set the ba	ndwidth of the tunnel interface:
	1	· /	

```
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.

	no descriptio	'n
Syntax Description	description-no	<i>ame</i> Description of the Interface.
Command Default	None	
Command Modes	Interface Conf	iguration
Command History	Release	Modification
	Release	This command was
	4.2.0	introduced.
Usage Guidelines	Ta waa thia aar	nmand, you must be in a user gro

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

Task ID

Task
IDOperationinterfaceread,
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

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	ith 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		r group assignment is preventin	group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator
Task ID	Task Opera ID	tions	
	network read, write		

 Task ID
 Operations

 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. None **Command Default** Interface configuration **Command Modes Command History** Release Modification Release 4.2.1 This command was introduced. To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. Task ID Task Operations ID network read,

write

Task ID	Operations
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]}

zone prefix length link-local route-tag value None nterface confi	Specifies the IPv6 address Specifies the length of the I Specifies the link-local add Specifies the tag associated Tag value. The range is from	Pv6 address prefix, in bits. The range is from 1 to 128. ress. with the address.
link-local route-tag value	Specifies the link-local add Specifies the tag associated	with the address.
route-tag value None	Specifies the tag associated	with the address.
value		
Jone	Tag value. The range is from	n 1 to 4294967295.
nterface confi		
·	guration	
Release	Modification	_
Release 4.2.1	This command was introduced.	_
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
Task ID Opera	tions	
network read, write		
	elease 4.2.1 o use this com os. If the user r assistance. ask ID Opera etwork read,	This command was introduced. b use this command, you must be in a user g b. If the user group assignment is prevention r assistance. ask ID Operations etwork read,

Task IDOperationsinterfaceread,
writeipv6read,
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	<i>size</i> Size of the MTU in bytes. The range is from 1280 to 65535.				
Command Default	None			-	
Command Modes	Interface con	figuration			
Command History	Release	Modification			
	Release 4.2.	1 This command was introduced.			
Usage Guidelines		er group assignment is pr	user group associated with eventing you from using a c		
Task ID	Task ID Ope	rations			
	network read wri	·			
	interface read wri	·			
	ipv6 read wri	·			

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.

unreachable. The default is 3 retries. The minimum value is 1 retry.

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

Command Default None

Command Modes interface configuration

Command History	Release Modification		
	Release 4.2.0	This command was introduced.	

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

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

)	Task ID	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	

Interface configuration **Command Modes**

Command History	Release	Modification
	Release 4.2.0	This command was introduced.

To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** 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	e configurati	on	
Command History	Release	e Modif	ication	
	Release 4.2.0	This c introd	command was luced.	
Usage Guidelines		ne user grouj		er group associated with a task group that includes appropriate task nting you from using a command, contact your AAA administrator
Task ID	Task ID	Operation		
	interface	read, write		
	This exa	mple 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 destinati	on is specified.
		tination ip-address destination ip-address	
Syntax Description	ip-address	Specifies the IPv4 or IPv6 address of the host of	lestination.
Command Default	None		
Command Modes	interface co	nfiguration	
Command History	Release	Modification	
	Release 4.2.0	This command was introduced.	

I

	Release	Modification		
	Release 5.2.2	The tunnel destinatio	n can be an IPv6 address.	
Usage Guidelines		user group assignment is	in a user group associated with a task group that includes appropriate task preventing you from using a command, contact your AAA administrator	
Task ID	Task ID ()perations		
	interface r	ead, vrite		
Examples	The following example shows how to configure interface tunnel:			
	RP/0/RSP0	. 3.	re # interface tunnel-ip 400 f)# tunnel destination 10.10.10.1	
Related Commands	Command		Description	
	tunnel mo	de, on page 34	Configures the encapsulation mode of the tunnel interface.	
			Cate a turnel interfecele course address	

tunnel mode, on page 34	configures the encapsulation mode of the turner interface.
tunnel source, on page 35	Sets a tunnel interface's source address.
tunnel tos, on page 36	Specifies the value of the TOS field in the tunnel encapsulating packets.
tunnel ttl, on page 37	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	<i>key-value</i> Specifies the tunnel key value. Range is from 0 to 4294967295.		
Command Default	No value is configured.		
Command Modes	interface configuration		

				-
Command History	Release	Modif	ication	
	Release 5.1.1	This c	ommand was introduced	-
Usage Guidelines		e user group		roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
		•		y on Cisco ASR 9000 Enhanced Ethernet line cards. It is the cards as Enhanced Ethernet line cards.
				vith tunnel key. If the configuration for the GRE keepalives and he tunnel is brought down and a warning message is displayed.
	• For	a given rout	ter, either the same key of	r different keys can be configured under multiple GRE tunnels.
		erent traffic hat tunnel.	streams passing throug	the same GRE tunnel contain the same GRE key configured
Task ID	Task ID	Operation		
	interface	read, write		
	tunnel	read, write		
	This exa	nple shows	how to configure the tu	nel key value at the GRE transmitter and receiver end:
	RP/0/RSI RP/0/RSI RP/0/RSI RP/0/RSI RP/0/RSI RP/0/RSI	20/CPU0:ro 20/CPU0:ro 20/CPU0:ro 20/CPU0:ro 20/CPU0:ro	uter# configure uter(config)# interf uter(config-if)#ipv4 uter(config-if)# tun uter(config-if)# tun uter(config-if)# tun	address 101.0.9.1 255.255.255.0 mel key 10

!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
 This command was introduced.

 5.1.1

Usage Guidelines

To use this command, you must be in a user group associated with a task 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 | copy}
no tunnel dfbit
```

Syntax Description	_		
Syntax Description	disable	Disables the DF bit in the o	uter packet. This allows the outer packet to be fragmented, if required.
	copy	Copies the DF bit value fro	m the inner packet to the outer packet.
		lote This is valid only	for an IPv4 transport network in an IP in IP tunnel.
Command Default	The DF b	value in the outer packet is	s disabled. This allows outer packet fragmentation, if required.
Command Modes	interface	nfiguration	
Command History	Release	Modification	
	Release 4.2.0	This command was intro	oduced.
	Release 5.3.1	The copy option is sup	ported.
Usage Guidelines		ser group assignment is pr	a user group associated with a task group that includes appropriate task eventing you from using a command, contact your AAA administrator
	network i		her packet to the outer packet is only supported for an IPv4 transport option is configured, you cannot configure an IP in IP tunnel over an
Task ID	Task ID	perations	
	interface	ead, rite	
Examples	The follo	ng example shows how to	enable fragmentation over an interface tunnel.

	RP/0/RSP0/CPU0:router# configur RP/0/RSP0/CPU0:router(config)# RP/0/RSP0/CPU0:router(config-if	nterface tunnel-ip 400 # tunnel dfbit disable Description Specifies a tunnel interface's destination address.		
Related Commands	Command	Description		
	tunnel destination, on page 29	Specifies a tunnel interface's destination address.		
	tunnel mode, on page 34	Configures the encapsulation mode of the tunnel interface.		
	tunnel source, on page 35	Sets a tunnel interface's source address.		

tunnel tos, on page 36Specifies the value of the TOS field in the tunnel encapsulating
packets.tunnel ttl, on page 37Configures 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.

Syntax Description	_		
Syntax Description	gre	ipv4	Specifies the tunnel as a GRE tunnel over an IPv4 transport network.
	gre	ipv6	Specifies the tunnel as a GRE tunnel over an IPv6 transport network.
	ipv4		Specifies the tunnel as an IP in IP tunnel over an IPv4 transport network.
	ipv6		Specifies the tunnel as an IP in IP tunnel over an IPv6 transport network.
Command Default	The default	t tunnel mode is set as a GRE tunnel over an IPv4 transpo	ort network.
Command Modes	interface co	onfiguration	
Command History	Release	Modification	-
	Release 4.2.0	This command was introduced.	-

VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers, IOS XR Release 6.4.x

	Release	Modification			
	Release 5.2.2	Support for GRE tunne	el on an IPv6 transport network.		
	Release 5.3.1	Support for IP in IP tu	mels.		
Usage Guidelines		iser group assignment is pl	a user group associated with a task group that includes appropriate task reventing you from using a command, contact your AAA administrator		
Task ID	Task ID 0	perations			
	interface re w	ead, rrite			
Examples	The following example shows how to configure interface tunnel:				
	RP/0/RSP0/	. 2.	e interface tunnel-ip 400)#tunnel mode gre ipv4		
Related Commands	Command		Description		
	tunnel dest	tination, on page 29	Specifies a tunnel interface's destination address.		
	tunnel sou	rce, on page 35	Sets a tunnel interface's source address.		
	tunnel tos,	on page 36	Specifies the value of the TOS field in the tunnel encapsulating packets.		
	tunnel ttl, o	n page 37	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 of	or IPv6 address to use as the source address for packets in the tunnel.
Command Default	None		
Command Modes	interface con	nfiguration	
Command History	Release	Modification	
	Release 4.2.0	This command was int	troduced.
	Release 5.2.2	The tunnel source can	be an IPv6 address.
Usage Guidelines		ser group assignment is p	a user group associated with a task group that includes appropriate task reventing you from using a command, contact your AAA administrator
	interface ID		tree is identified using the interface ID and not the IP address. Using the k the tunnel as down when the interface is down and the routing protocol e to the tunnel route.
Task ID	Task ID Op	perations	
	interface rea	ad, rite	
Examples	The following	ng example shows how to	o configure interface tunnel:
	RP/0/RSP0/		re interface tunnel-ip 400)# tunnel source 10.10.10.1
Related Commands	Command		Description
	tunnel desti	nation, on page 29	Specifies a tunnel interface's destination address.
	tunnel mod	e, on page 34	Configures the encapsulation mode of the tunnel interface.
	tunnel tos, o	on page 36	Specifies the value of the TOS field in the tunnel encapsulating packets.
	tunnel ttl, or	n page 37	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 no tunnel	tos_value tos_tos_value			
Syntax Description	<i>tos_value</i> Specifies the value of the TOS field in the tunnel encapsulating packets. The TOS value ranges between 0 to 255.				
Command Default	-	TOS/COS bits of the inter ied to TOS bits of the GR	rnal IP header to the GRE IP header. In case of labeled payload, EXP E IP header.		
Command Modes	interface co	onfiguration			
Command History	Release	Modification			
	Release 4.2.0	This command was introduced.			
Usage Guidelines		user group assignment is p	a user group associated with a task group that includes appropriate task reventing you from using a command, contact your AAA administrator		
Task ID	Task Op ID	perations			
	interface re	ad, rite			
Examples	The followi	ing example shows how to	o configure interface tunnel:		
	RP/0/RSP0/	/CPU0:router# configur /CPU0:router(config)# /CPU0:router(config-if	interface tunnel-ip 400		
Related Commands	Command		Description		
	tunnel des	tination, on page 29	Specifies a tunnel interface's destination address.		
	tunnel mod	le, on page 34	Configures the encapsulation mode of the tunnel interface.		
	tunnel sou	rce, on page 35	Sets a tunnel interface's source address.		
	tunnel ttl, c	on page 37	Configures the Time-To-Live (TTL) for packets entering the tunnel.		

tunnel ttl

I

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 no tunnel	ttl_value ttl_ttl_value	
Syntax Description		Specifies the value of TTL for pa 255.	ackets entering the tunnel. The TTL value ranges between 1 to
Command Default	The default	TTL value is set to 255.	
Command Modes	interface co	nfiguration	
Command History	Release	Modification	_
	Release 4.2.0	This command was introduced.	_
Usage Guidelines		iser group assignment is prevent	group associated with a task group that includes appropriate task ing you from using a command, contact your AAA administrator
		and specifies the Time-To-Live f arrier network before reaching the	for packets entering the tunnel so that the packets are not dropped he tunnel destination.
Task ID	Task Op ID	perations	
	interface re	ad, rite	
Examples	The followi	ng example shows how to confi	gure interface tunnel:
	RP/0/RSP0/	<pre>'CPU0:router# configure 'CPU0:router(config)# inte 'CPU0:router(config-if)#tur</pre>	rface tunnel-ip 400 nnel source 10.10.10.1
Related Commands	Command		Description
	tunnel dest	tination, on page 29	Specifies a tunnel interface's destination address.
	tunnel mod	le, on page 34	Configures the encapsulation mode of the tunnel interface.
	tunnel tos,	on page 36	Specifies the value of the TOS field in the tunnel encapsulating packets.
	tunnel sou	rce, on page 35	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 43
- address-family 12vpn mspw, on page 43
- bgp, on page 44
- backup (L2VPN), on page 45
- backup disable (L2VPN), on page 46
- clear l2vpn collaborators, on page 47
- clear l2vpn counters bridge mac-withdrawal, on page 48
- clear l2vpn forwarding counters, on page 49
- clear l2vpn forwarding counters bridge-domain mirp-lite, on page 50
- clear l2vpn forwarding message counters, on page 51
- clear l2vpn forwarding table, on page 52
- control-word, on page 52
- dynamic-arp-inspection, on page 53
- flood mode, on page 55
- generic-interface-list, on page 56
- global-id (L2VPN), on page 57
- interface (p2p), on page 58
- interworking ipv4, on page 59
- ipv4 source, on page 60
- 12tp static, on page 61
- ip-source-guard, on page 63
- l2transport, on page 64
- l2transport l2protocol, on page 66
- l2transport propagate, on page 67
- l2transport service-policy, on page 68
- l2vpn, on page 69
- load-balancing flow, on page 70
- load-balancing pw-label, on page 71
- logging (l2vpn), on page 72

- logging nsr, on page 73
- monitor-session (l2vpn), on page 74
- mpls static label (L2VPN), on page 75
- neighbor (L2VPN), on page 76
- neighbor evpn, on page 79
- neighbor routed, on page 79
- nsr (L2VPN), on page 80
- pw-routing, on page 81
- preferred-path, on page 82
- protocol l2tpv3, on page 83
- pw-class (L2VPN), on page 84
- pw-class encapsulation l2tpv3, on page 85
- pw-class encapsulation mpls, on page 87
- pw-ether, on page 89
- pw-grouping, on page 91
- p2p, on page 92
- rd (L2VPN), on page 93
- sequencing (L2VPN), on page 94
- show bgp l2vpn evpn, on page 95
- show bgp l2vpn mspw, on page 97
- show bgp vrf-db, on page 98
- show evpn evi ead, on page 99
- show evpn internal-label, on page 100
- show dci-fabric-interconnect, on page 101
- show generic-interface-list, on page 103
- show l2tp session, on page 105
- show l2tp tunnel, on page 106
- show l2vpn, on page 108
- show l2vpn atom-db, on page 110
- show l2vpn collaborators, on page 112
- show l2vpn database, on page 113
- show l2vpn discovery, on page 115
- show l2vpn forwarding, on page 117
- show l2vpn forwarding message counters, on page 130
- show l2vpn generic-interface-list, on page 132
- show l2vpn index, on page 133
- show l2vpn nsr, on page 135
- show l2vpn process fsm, on page 136
- show l2vpn provision queue, on page 138
- show l2vpn pw-class, on page 139
- show l2vpn pwhe, on page 141
- show l2vpn resource, on page 142
- show l2vpn trace, on page 143
- show l2vpn xconnect, on page 145
- show tech-support l2vpn platform no-statistics, on page 157
- source (p2p), on page 158

- storm-control, on page 159
- tag-impose, on page 161
- tos (l2vpn), on page 162
- transport mode (L2VPN), on page 164
- transport mode vlan passthrough, on page 165
- ttl (l2vpn), on page 166
- xconnect group, on page 167

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-r	nac		
Syntax Description	This comm	and 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		user group assignment is preventing	-	a task group that includes appropriate task command, contact your AAA administrator
	The follow	ing example shows how to advertis	e local MAC.	
	RP/0/RSP0, RP/0/RSP0, RP/0/RSP0,	/CPU0:router# configure /CPU0:router(config)# evpn /CPU0:router(config-evpn)# ev: /CPU0:router(config-evpn-evi);	pdb	cy spp-basic-6

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	keyword	s 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 12vpn 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 rou	ting configuration submode	
Command History	Release	Modification	
	Release 5.1.2	This command was introduced.	
Usage Guidelines		command, you must be in a user gro	

Jsage Guidelines To use this command, you must be in a user group associated with a task 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	
	pw-id valı	<i>ue</i> Configures the pseudowire ID. The range is from 1 to 4294967295.
Command Default	None	
Command Modes	L2VPN xco	connect p2p pseudowire configuration
Command History	Release	Modification
	Release 3.7.2	This command was introduced.
Usage Guidelines		command, you must be in a user group associated with a task group that includes appropriate task user group assignment is preventing you from using a command, contact your AAA administrator nce.
	Use the bac	ckup command to enter L2VPN xconnect p2p pseudowire backup configuration mode.
Task ID	Task Ope ID	perations
	l2vpn rea wr	
Examples	The follow	ring example shows how to configure backup pseudowires:
	RP/0/RSP0, RP/0/RSP0,	/CPU0:router# configure /CPU0:router(config)# 12vpn /CPU0:router(config-12vpn)# xconnect group gr1 /CPU0:router(config-12vpn-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 46	Specifies how long a backup pseudowire should wait before resuming operation after the primary pseudowire goes down.	
	l2vpn, on page 69	Enters L2VPN configuration mode.	
	neighbor (L2VPN), on page 76	Configures a pseudowire for a cross-connect.	
	p2p, on page 92	Enters p2p configuration submode to configure point-to-point cross-connects.	
	xconnect group, on page 167	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	delaySpecifies 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 t	o 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 pse	eudowire class configuration		
Command History	Release	Modification		
	Release 3.7	7.2 This command was introduced.		
Usage Guidelines		iser group assignment is preventing	oup associated with a task group that includes appropriate task you from using a command, contact your AAA administrator	

Task ID	Task ID	Operations	
	l2vpn	read, write	
Examples		-	shows how a backup delay is configured for point-to-point pseudowire in le delay is set to 50 seconds:
	RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R	SP0/CPU0:ro SP0/CPU0:ro SP0/CPU0:ro SP0/CPU0:ro SP0/CPU0:ro SP0/CPU0:ro SP0/CPU0:ro SP0/CPU0:ro	<pre>er# configure er(config)# l2vpn er(config-l2vpn)# pw-class class1 er(config-l2vpn-pwc)# backup disable delay 50 er(config-l2vpn-pwc)# exit er(config-l2vpn)# xconnect group A er(config-l2vpn-xc)# p2p rtrx er(config-l2vpn-xc-p2p)# neighbor 10.1.1.1 pw-id 2 er(config-l2vpn-xc-p2p-pw)# pw-class class1 er(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5 er(config-l2vpn-xc-p2p-pw-backup)#</pre>
Related Commands	Comm	and	Description
	l2vpn,	on page 69	Enters L2VPN configuration mode.
	neighb	or (L2VPN), o	age 76 Configures a pseudowire for a cross-connect.
	p2p, on page 92		Enters p2p configuration submode to configure point-to-poin cross-connects.
	pw-cla	ass (L2VPN), c	age 84 Enters pseudowire class submode to define a pseudowire class submode to define a pseudowire class template.
	xconn	ect group, on	ge 167 Configures cross-connect groups.

clear l2vpn collaborators

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

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.

clear l2vpn collaborators

To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. Task ID Task **Operations** ID l2vpn read, write **Examples** The following example shows how to clear change counters for L2VPN collaborators: RP/0/RSP0/CPU0:router# clear 12vpn collaborators **Related Commands** Command Description show I2vpn collaborators, on page 112 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 | neighbor ip-address pw-id value}

Syntax Description	all	Clears the MAC withdrawal statistics over all the bridges.
	group group-na	me Clears the MAC withdrawal statistics over the specified group.
	bd-name bd-name	ne Clears the MAC withdrawal statistics over the specified bridge.
	neighbor <i>ip-address</i>	Clears the MAC withdrawal statistics over the specified neighbor.
	pw-id value	Clears the MAC withdrawal statistics over the specified pseudowire. The range is from 1 to 4294967295.
Command Default	None	
Command Modes	EXEC	
Command History	Release N	odification
		his command was troduced.

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

Task IDTask OperationsID12vpn read,
write

Examples

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

RP/0/RSP0/CPU0:router# clear 12vpn counters bridge mac-withdrawal all

clear l2vpn forwarding counters

clear l2vpn forwarding counters

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

	cicui 12		irung counters			
Syntax Description	This cor	This command has no arguments or keywords.				
Command Default	None					
Command Modes	EXEC					
Command History	Release	e Mod	ification	-		
	Release	e 3.7.2 This	command was introduced.	-		
Usage Guidelines		he user grou	d, you must be in a user gr p assignment is preventing			
Task ID	Task ID	Operations				
	l2vpn	read, write				
Examples	The folle	owing exam	ple shows how to clear L2	VPN forwardin	g counters:	

VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers, IOS XR Release 6.4.x

RP/0/RSP0/CPU0:router# clear 12vpn forwarding counters

Related Commands	Command	Description
	show I2vpn forwarding, on page 117	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 <i>node-id</i> Clears the L2VPN forwarding MIRP counters for the specified location.						
Command Default	None						
Command Modes	EXEC						
Command History	Release	Modificatio	n				
	Release 4.3.0	This comm introduced.					
Usage Guidelines		user group assig	must be in a user gr gnment is preventin	-	-		
Task ID	Task Op ID	eration	_				
	l2vpn rea	ad, write, ecute	_				
	This examp	ple shows how	– to clear all the MIR	P counters:			
	RP/0/RSP0 0/1/CPU0	/CPU0:router#	clear 12vpn for	warding coun	ters bridge-do	main mirp-lite	location

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 49	Clears L2VPN forwarding counters.		

clear I2vpn 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 forwardin	g message counters for the specified location.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 3.7.2	This command was introduce	ed.
Usage Guidelines		er group assignment is prevent	group associated with a task group that includes appropriate task ing you from using a command, contact your AAA administrator
Task ID	Task Oper ID	ations	
	l2vpn read write		
Examples	The following node:	g example shows how to clear	L2VPN forwarding message counters on a specified
	RP/0/RSP0/C	PUO:router# clear 12vpn f	orwarding message counters location 0/6/CPU0
Related Commands	Command		Description
	show l2vpn f	orwarding, on page 117	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 Clears L2VPN forwarding tables for the specified location. node-id Image: Clear state of the specified location.			
Command Default	None			
Command Modes	EXEC			
Command History	Release	Modification	_	
	Release 3.9.0) This command was introduce	d.	
Usage Guidelines		er group assignment is preventi	group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator	
Task ID	Task Oper ID	rations		
	l2vpn read writ			
Examples	The followin	g example shows how to clear	an L2VPN forwarding table from a specified location:	
	RP/0/RSP0/C	PU0:router# clear l2vpn fc	rwarding table location 1/2/3/5	
Related Commands	Command		Description	
	show l2vpn f	orwarding, on page 117	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 Operations ID		
	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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# pw-class pwc1 RP/0/RSP0/CPU0:router(config-12vpn-pwc)# encapsulation mpls RP/0/RSP0/CPU0:router(config-12vpn-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	(Optiona	al) 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	n (Optiona	al) Performs address-validation.

	src-mac S	Source MAC address in the Ethernet header.		
	dst-mac I	Destination MAC address in the Ethernet header.		
	ipv4 I	P addresses in the ARP body.		
Command Default	Dynamic ARP inspect	ion is disabled.		
Command Modes	l2vpn bridge group bri	dge domain configuration		
Command History	Release Modifie	cation		
	Release 4.0.1 This co introdu			
Usage Guidelines		you must be in a user group associated with a task group that includes appropriate task assignment is preventing you from using a command, contact your AAA administrator		
Task ID	Task Operations ID			
	l2vpn read, write			
Examples	This example shows h	ow to enable dynamic ARP inspection on bridge bar:		
	RP/0/RSP0/CPU0:rout	-		
	RP/0/RSP0/CPU0:router (config=12vpn-bg-bd-dai) # This example shows how to enable dynamic ARP inspection logging on bridge bar:			
	RP/0/RSP0/CPU0:rout RP/0/RSP0/CPU0:rout RP/0/RSP0/CPU0:rout	-		
		-		

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 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	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}

resilience-optimized Configures bridge to		Configures bridge to use Resilience Optimized mode.
convergence-	optimized	Configures bridge to use Convergence Optimized mode.
The bridge do	main opera	tes in the Bandwidth Optimized Mode.
l2vpn bridge g	group bridge	e domain configuration
mand History Release Modification		ion
Release 3.7.2	This com	
-	convergence The bridge do l2vpn bridge g Release	convergence-optimized The bridge domain opera l2vpn bridge group bridge Release Modificat Release 3.7.2 This commit

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

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

е

Task ID	Task Operat ID	ions				
	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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group MyGroup RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain MyDomain RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# flood mode convergence-optimized RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)#					
Related Commands	Command		Description			
	l2vpn, on page	e 69	Enters L2VPN configuration mode.			
	bridge-domai	n (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.			
	bridge group	(VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and			

generic-interface-list

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

then to assign network interfaces to the bridge domain.

Syntax Description	list-name	Name of the interface list.
Command Default	None	
Command Modes	Global con	figuration
Command History	Release	Modification
	Release 4.2.1	This command was introduced.

generic-interface-list list-name

to compare generic metrace ist, use the generic-internate inst command in global comparation in

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

Task ID Task ID

> l2vpn read, write

Operation

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

. C

Command	Description
show I2vpn generic-interface-list, on page 132	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	<i>value</i> 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			
	ReleaseThis command was introduced.5.1.2			
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate tas IDs. If the user group assignment is preventing you from using a command, contact your AAA administrate for assistance.			
	This command overwrites the AS number from BGP.			

Task ID Task Operation ID

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 type interface-path-id [**PW-Ether** | **PW-IW**] **no interface** type interface-path-id [**PW-Ether** | **PW-IW**]

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.

Syntax Description	<i>type</i> Interface type. For more information, use the question mark (?) online help function.					
	<i>interface-path-id</i> Physical interface or a virtual interface.					
	v 1	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.				
	PW-Ether (Optional) Configures an Ethernet Interface.					
	PW-IW (Optional) Configures an IP Interworking Interface.					
Command Default	None					
Command Modes	p2p configuration	on submode				
Command History	Release	Modification				
	Release 3.7.2	This command was introduced.				
	Release 4.2.1	The following keywords were added:				
		• PW-Ether				
		• PW-IW				

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
Task ID	Task ID	Operations	
	l2vpn	read, write	
Examples	RP/0/R RP/0/R RP/0/R	SP0/CPU0:router SP0/CPU0:router SP0/CPU0:router	hows how to configure an attachment circuit on a TenGigE interface: # configure (config) # 12vpn (config-12vpn) # xconnect group gr1 (config-12vpn-xc) # p2p p001
	RP/0/R	SP0/CPU0:router	<pre>(config-l2vpn-xc-p2p) # interface TenGigE 1/1/1/1</pre>
Related Commands	Comma	and	Description
	p2p, or	n page 92	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	Release	Modification	
	Release 4.0.0	This command was introduced.	
Usage Guidelines	To use this	command, you must be in a user g	

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

I

Task ID	Task ID	Operations				
	l2vpn	read, write				
Examples	The fol	lowing examp	le shows how to configure an attachment circuit on a TenGigE interface:			
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# 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	Comm	and	Description			
	p2p, oi	n page 92	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	e source-ip-address	
Syntax Description	source-ip-ad	ddress Source IP address.	_
Command Default	None		
Command Modes	L2VPN pseu	dowire class encapsulatio	n mpls configuration
Command History	Release	Modification	
	Release 4.2.0	This command was introduced.	
Usage Guidelines		ser group assignment is pro	user group associated with a task group that includes appropriate task eventing you from using a command, contact your AAA administrator
Task ID	Task Oper ID	ration	
	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)#12vpn
RP/0/RSP0/CPU0:router(config-12vpn)#pw-class kant1
RP/0/RSP0/CPU0:router(config-12vpn-pwc)#encapsulation mpls
RP/0/RSP0/CPU0:router(config-12vpn-pwc-mpls)#ipv4 source 112.22.1.4
```

Related Commands	Command	Description
	pw-class encapsulation mpls, on page 87	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.

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					
	ReleaseThis command was4.3.1introduced					
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.					
Task ID	Task Operation ID					
	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)# 12vpn xconnect group 12vpn RP/0/RSP0/CPU0:router(config-12vpn-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)# 12tp static					
	This example shows how to configure local and remote session-id:					
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn xconnect group 12vpn RP/0/RSP0/CPU0:router(config-12vpn-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)# 12tp static local session 1 RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# 12tp 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)# 12vpn xconnect group 12vpn RP/0/RSP0/CPU0:router(config-12vpn-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)# 12tp static local cookie size 0 RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# 12tp static remote cookie size 0					
	This example is with cookie size 4:					
	<pre>RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn xconnect group 12vpn RP/0/RSP0/CPU0:router(config-12vpn-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)# 12tp static local cookie size 4 value <0x0-0xffffffff</pre>					

RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# l2tp static remote cookie size 4 value
<0x0-0xffffffff</pre>

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)# 12vpn xconnect group 12vpn
RP/0/RSP0/CPU0:router(config-12vpn-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)# 12tp static local cookie size 8 value
<0x0-0xffffffff <0x0-0xffffffff>
RP/0/RSP0/CPU0:router(config-xc-p2p-pw)# 12tp static remote cookie size 8 value
<0x0-0xfffffffff <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</pre>
```

Related Commands	Command	Description
	l2vpn, on page 69	Enters L2VPN configuration mode.
	p2p, on page 92	Enters p2p configuration submode to configure point-to-point cross-connects.
	xconnect group, on page 167	Configures cross-connect groups.
	neighbor (L2VPN), on page 76	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	Releas	se l	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 appr IDs. If the user group assignment is preventing you from using a command, contact your AAA as for assistance.				
Task ID	Task ID	Operatio	ns		
	l2vpn	read, write	_		
Examples	This ex	ample sł	nows how to enable ip s	ource guard on bridge bar:	
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group b1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# ip-source-guard RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-ipsg)#				
	This example shows how to enable ip source guard logging on bridge bar:				
	<pre>RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group b1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# ip-source-guard logging RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-ipsg)#</pre>				
Related Commands	Comma	and		Description	
	bridge	-domain	(VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.	
	bridge	group (V	(PLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.	

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.

Enters L2VPN configuration mode.

l2transport no l2transport

l2vpn, on page 69

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 Operations ID				
	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)# 12transport				
	Ethernet VLAN Mode:				
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0.900 12transport 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 dotlq 20 second-dotlq 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 I2vpn forwarding, on page 117	Displays forwarding information from the layer2_fib manager on the line card.	

I2transport I2protocol

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

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 include	s 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 Examples	Task ID	Operations			
	l2vpn	read, write			
	atm	read, write			
	The following example shows how to configure Layer 2 protocol handling:				
	RP/0/R	SP0/CPU0:rout		nterface GigabitEthernet 0/0/0/0 # 12transport 12protocol cpsv reverse-tunnelstp drop	
Related Commands	Comm	and		Description	
	show	2vpn forwardin	g, on page 117	Displays forwarding information from the layer2_fib manager on the line card.	

I2transport 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 conf	figuration			
Command History	Release	Modification			
	Release 3.7.2	2 This command was introduced.			
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.				
	The l2transport propagate command provides a mechanism for the detection and propagation of remote link failure for port mode EoMPLS.				
	To display the state of l2transport events, use the show controller internal command in <i>Interface and Hardware Component Configuration Guide for Cisco ASR 9000 Series Routers</i>				
	For more information about the Ethernet remote port shutdown feature, see <i>MPLS Configuration Guide for Cisco ASR 9000 Series Routers</i> .				
Task ID	Task Opera ID	tions			
	l2vpn read, write				
Examples	The following example shows how to propagate remote link status changes:				
	RP/0/RSP0/CI		erface GigabitEthernet 0/0/0/0 12transport propagate remote remote-status		
Related Commands	Command		Description		
	show l2vpn fo	orwarding, on page 117	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.

12transport service-policy {input policy-name | output policy-name} no 12transport service-policy {input policy-name | output policy-name}

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

	output Configures the direction of service policy application: output. policy-name			
Command Default	None			
Command Modes	Interface configuration			
Command History	Release Modification			
	Release 3.7.2 This command was introduced.			
Usage Guidelines		user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator		
Task ID	Task Operations ID			
	l2vpn read, write			
	atm read, write			
Examples	The following example shows how configure an L2 transport quality of service (QoS) policy:			
		pure # interface GigabitEthernet 0/0/0/0 if)# 12transport service-policy input sp_0001		
Related Commands	Command	Description		
	show l2vpn forwarding, on page 117	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

I

Command Modes	Global config	guration	
Command History	Release Modification		
	Release 3.7.	2 This command was introduce	ed.
Usage Guidelines		er group assignment is prevent	group associated with a task group that includes appropriate task ing you from using a command, contact your AAA administrator
Note	All L2VPN c	configuration can be deleted us	ing the no l2vpn command.
Task ID	Task Ope ID	rations	
	l2vpn read writ		
Examples	The followin	g example shows how to enter	L2VPN configuration mode:
	RP/0/RSP0/C	CPU0:router# configure CPU0:router(config)# 12vpn CPU0:router(config-12vpn)#	
Related Commands	Command		Description
	show l2vpn f	forwarding, on page 117	Displays forwarding information from the layer2_fib manager on the line card.

load-balancing flow

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

	load-balancing flow [{src-dst-mac src-dst-ip}]			
Syntax Description	src-dst-mac Enables global flow load balancing hashed on source and destination MAC addr	esses.		
	src-dst-ip Enables global flow load balancing hashed on source and destination IP address	ses.		
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 Operations ID
	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)# 12vpn

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

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 comm	This command has no arguments or keywords.			
Command Default	None	None			
Command Modes	Pseudowire class configuration				
Command History	Release	Modification	_		
	Release 4.0	0.0 This command was introduced.	_		
Usage Guidelines		user group assignment is preventi	group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator		
Task ID	Task Ope ID	erations			
	l2vpn rea wri				

Examples

The following example shows how to set the bridge ID:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# pw-class abc
RP/0/RSP0/CPU0:router(config-12vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:router(config-12vpn-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 Operations ID		
	l2vpn read, write		
Examples	The following example shows how to enable cross-connect logging:		
	RP/0/RSP0/CPU0:router# configure		

<pre>RP/0/RSP0/CPU0:router(config)# 12vpn</pre>		
RP/0/RSP0/CPU0:router(config-l2vpn)#	logging pseudowire	status

Related Commands	Command	Description
	l2vpn, on page 69	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 no log	g nsr ging nsr			
Syntax Descrip	tion	This co	This command has no keywords or arguments.			
Command Defa	ult	None				
Command Mod	es	L2VPN	configuratio	n submode		
Command Histo	ory	Releas	e Modif	ication		
		Releas 4.3.0	e This c	ommand was introduced.		
Usage Guidelin	es		the user group		oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator	
-	Note	All L2V	/PN configur	ation can be deleted using	g the no l2vpn command.	
Task ID		Task ID	Operations			
		l2vpn	read, write			
Examples		The fol	lowing exam	ple shows how to enable	non-stop routing logging:	
		RP/0/R	SP0/CPU0:ro	uter# configure		

<pre>RP/0/RSP0/CPU0:router(config) # 13</pre>	2vpn
RP/0/RSP0/CPU0:router(config-12v)	pn)# logging nsr

Related Commands	Command	Description
	l2vpn, on page 69	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 defa	No default behavior or values		
Command Modes	Point-to	Point-to-point cross connect configuration		
Command History	Releas	e Ma	odification	-
	Release	e 4.0.0 Th	is command was introduced.	-
Usage Guidelines	global c point-to connect associat the cros	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 <i>session-name</i> argument should be different than any interface names currently used in the system.		
Task ID	Task ID	Operations	S	
	l2vpn	read, write	_	
Examples	This ex	ample show	— ws how to attach a traffic mi	rroring session as segment for the xconnect:
	RP/0/RS RP/0/RS	SP0/CPU0:: SP0/CPU0::	router(config)# 12vpn router(config-12vpn)# x (router(config-12vpn-xc) router(config-12vpn-xc-p	

This example shows how an EFP is associated to a monitor session:

```
RP/0/RSP0/CPU0:router(config)# interface Gi0/0/0/4.2 l2transport
RP/0/RSP0/CPU0:router(config-subif) # monitor-session customer-foo
```

This example shows how L2 SPAN is supported on L3 interfaces, but the whole L2 frame is mirrored:

```
RP/0/RSP0/CPU0:router(config) # interface Gi0/0/0/4.2 l2transport
RP/0/RSP0/CPU0:router(config-subif)# ipv6 address 1111:3333::cdef
RP/0/RSP0/CPU0:router(config-subif) # monitor-session customer-foo
```

This example shows how SPAN is also supported on main interfaces:

```
RP/0/RSP0/CPU0:router(config)# interface Gi0/0/0/4.2 l2transport
RP/0/RSP0/CPU0:router(config-subif) # 12transport
RP/0/RSP0/CPU0:router(config-subif) # monitor-session customer-foo
```

This example shows creation of xconnect between the monitor-session and a L2TPv3 over IPv6 tunnel:

```
RP/0/RSP0/CPU0:router(config) # 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# xconnect group span
RP/0/RSP0/CPU0:router(config=l2vpn-xc) # p2p span-foo
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# monitor-session customer-foo
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# neighbor ipv6 1111:3333::cdef pw-id 1001
RP/0/RSP0/CPU0:router(config-12vpn-xc-p2p-pw)# pw-class ts
RP/0/RSP0/CPU0:router(config-12vpn-xc-p2p-pw)# source 1111:3333::abcd
RP/0/RSP0/CPU0:router(config-12vpn-xc-p2p-pw)# 12tp static local cookie size 8 value 0xabcd
 0x1234
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# 12tp static remote cookie size 8 value 0xcdef
 0x5678
```

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 no mpls static label local label remote value

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

Command Default	The default behavior is a dynamic label assignment.					
Command Modes	L2VPN cross-connect P2P pseudowire configuration					
Command History	Release Modification					
	Release 3.7	7.2 This co	ommand was introduce	ed.		
Usage Guidelines		iser group a		group associated with a task group that includes appropriate task ing you from using a command, contact your AAA administrator		
Task ID	Task Op ID	erations				
	l2vpn rea wr					
Examples	The following example shows how to configure static labels for MPLS L2VPN:					
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn xconnect group 12vpn RP/0/RSP0/CPU0:router(config-12vpn-xc)# p2p rtrA_to_rtrB RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000 RP/0/RSP0/CPU0:router(config-12vpn-xc-p2p-pw)# mp1s static label local 800 remote 500					
Related Commands	Command			Description		
	l2vpn, on page 69			Enters L2VPN configuration mode.		
	neighbor (L2VPN), on page 76		page 76	Configures a pseudowire for a cross-connect.		
	p2p, on pag	ge 92		Enters p2p configuration submode to configure point-to-point cross-connects.		
	xconnect group, on page 167			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 | ipv4 ipv4 address | ipv6 ipv6 address} pw-id value [{backup | l2tp static | mpls

 || pw-class | source ipv6 address | tag-impose}]

 no neighbor {A.B.C.D | ipv4 ipv4 address | ipv6 ipv6 address} pw-id value [{backup | l2tp static | mpls

 || pw-class | source ipv6 address | tag-impose}]

	ipv4 ipv4 address	Assigns the IPv4 address of the cross-connect peer.Assigns the IPv6 address of the cross-connect peer.Configures the pseudowire ID and ID value. Range is 1 to 4294967295.		
	ipv6 ipv6 address			
	pw-id value			
	backup	(Optional) Specifies the backup pseudowire for the cross-connect.		
	12tp static	(Optional) Configures the L2TP pseudowire static (Optional) Configures an MPLS static label.		
	mpls			
	pw-class	(Optional) Configures the pseudowire class template name to use for this cross-connect.		
	source ipv6 address	(Optional) Specifies the source IPv6 address of the pseudowire. This option is available only for the IPv6 neighbor.		
	tag-impose	(Optional) Specifies a tag during a VLAN ID configuration		
Command Default	None			
Command Modes	p2p configuration submode			
Command History	Release Modification			
	Release 3.7.2 This c	command was introduced.		
	Release 4.2.1 The ke	eyword tag-impose was introduced.		
	Release 4.3.1 The fo	ollowing keywords were added:		
	• iĮ	pv4		
	-	pv6		
		2tp static ource		
Usage Guidelines		, you must be in a user group associated with a task group that includes appropriate tasl assignment is preventing you from using a command, contact your AAA administrato		
	A cross-connect may	have two segments:		
	1. An Attachment C	fircuit (AC)		
	2. An second AC or	a pseudowire		
Note		entified by two keys: neighbor and pseudowire ID. There may be multiple pseudowires ghbor. It is not possible to configure only a neighbor.		
	All L 2VDN configurations can be delated using the ne l2vnn command			

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

Task ID	Task Operations ID					
	l2vpn read, write					
Examples	This example shows a point-to-point cross-connect configuration (including pseudowire configuration):					
	<pre>RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn xconnect group 12vpn RP/0/RSP0/CPU0:router(config-12vpn-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)# neighbor 10.2.2.3 pw-id 200 pw-class class23 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):</pre>					
	<pre>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</pre>					
	This example shows a point-to-point IPv6 cross-connect configuration:					
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn xconnect group 12vpn RP/0/RSP0/CPU0:router(config-12vpn-xc)# p2p rtrA_to_rtrB RP/0/RSP0/CPU0:router(config-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1					
	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)# 12vpn xconnect group 12vpn RP/0/RSP0/CPU0:router(config-12vpn-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)# source 1111:2222::abcd					

Command	Description	
l2vpn, on page 69	Enters L2VPN configuration mode.	
p2p, on page 92	Enters p2p configuration submode to configure point-to-point cross-connects.	
pw-class (L2VPN), on page 84	Enters pseudowire class submode to define a pseudowire class template.	
xconnect group, on page 167	Configures cross-connect groups.	
	l2vpn, on page 69 p2p, on page 92 pw-class (L2VPN), on page 84	

L

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-idtarget ac-id

Syntax Description	evi v _l	evi <i>vpn-id</i> Virtual Private Network Identifier where this p2p xconnect is setup.			
	target	ac-id S	Specifies the targeted remote attachment circuit id of the EVPN.		
Command Default	None				
Command Modes	p2p cor	nfiguratio	on submode		
Command History	Releas	se M	Iodification		
	Releas 6.0.0	e T	his command was introduced.		
Usage Guidelines		the user g	nand, you must be in a user group associated with a task group that includes appropriate task group assignment is preventing you from using a command, contact your AAA administrator		
Task ID	Task ID	Operati	 on		
	l2vpn	read, write			
		1			

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)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# xconnect group xc1
RP/0/RSP0/CPU0:router(config-12vpn-xc)# p2p vpws
RP/0/RSP0/CPU0:router(config-12vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
RP/0/RSP0/CPU0:router(config-12vpn-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 attac	hment circuit id.		
	source ac-id	Specifies the local attachment cire	cuit ID.		
Command Default	None				
Command Modes	p2p configurat	ion submode			
Command History	Release	Modification			
	Release 5.1.2	This command was introduced.			
Usage Guidelines		nmand, you must be in a user group group assignment is preventing yo		• • • • • •	-
Task ID	Task Opera ID	tion			
	l2vpn read, write				
	The following example shows how to enable pseudowire routing configuration submode for the p2p cross-connect.				
	RP/0/RSP0/CP RP/0/RSP0/CP RP/0/RSP0/CP RP/0/RSP0/CP RP/0/RSP0/CP	U0:router# configure U0:router(config)# l2vpn U0:router(config-l2vpn)# xcon U0:router(config-l2vpn-xc)# p2 U0:router(config-l2vpn-xc-p2p) U0:router(config-l2vpn-xc-p2p) U0:router(config-l2vpn-xc-p2p)	2p pw-ss)# interface gi)# neighbor rou	gabitethernet 0/1/0/9 ted 100:2.2.2.2:10 sourc	ce 10
nsr (L2VPI	N)				
	To configure n	on-stop routing, use the nsr comma	and in L2VPN cor	nfiguration submode. To retu	Irn 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		bled by default for L2VPN On Cis and under L2VPN configuration su	sco IOS XR 64 bit operating system. You cannot configure the bmode.			
Task ID	Task Op ID	peration				
	l2vpn rea	ad, rite				
	The following example shows how to configure non-stop routing:					
	RP/0/RSP0,	/CPU0:router# configure /CPU0:router(config)# 12vpn /CPU0:router(config-12vpn)# r	sr			
Related Commands	Command		Description			
	l2vpn, on p	age 69	Enters L2VPN configuration mode.			

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

 12vpn
 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 | tunnel-tp } value [fallback disable] no preferred-path interface { tunnel-ip | tunnel-te | tunnel-tp } value [fallback disable]

Syntax Description	interface	Interface for the preferred path.IP tunnel interface name for the preferred path.		
	tunnel-ip			
	value	Tunnel number for preferred path.		
	fallback disab	(Optional) Disables fallback for preferred path tunnel settings. Specifies the TE tunnel interface name for the preferred path.		
	tunnel te			
	tunnel tp	Specifies the TP tunnel interface name for the preferred path.		
Command Default	None			
Command Modes	Encapsulation N	MPLS configuration		
Command History	Release	Modification		
	Release 3.7.2	This command was introduced.		
	Release 4.2.0	The keyword tunnel-tp was introduced.		

Usage Guidelines	IDs. If for assi The pr e	the user group stance. eferred-path	p assignment is prev	ser group associated with a task group that includes appropriate task enting you from using a command, contact your AAA administrator able only to pseudowires with MPLS encapsulation. mmand to show the status of fallback (that is, enabled or disabled).
	0 se the	, snow 12 v pri		minand to show the status of randaek (that is, chaoled of disabled).
Note	All L2V	VPN configu	rations can be delete	d using the no l2vpn command.
Task ID	Task ID	Operations		
	l2vpn	read, write		
Examples	This ex	ample shows	s how to configure p	referred-path tunnel settings:
	RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R	SP0/CPU0:ro SP0/CPU0:ro SP0/CPU0:ro SP0/CPU0:ro	outer (config-12vpr outer (config-12vpr outer (config-12vpr	<pre>mpn)# pw-class kanata01pwc)# encapsulation mplspwc-encap-mpls)# preferred-path interface tunnel-tp 345pwc-encap-mpls)# preferred-path interface tunnel-tp 345</pre>
Related Commands	Comm	and		Description
	show I	2vpn xconne	ct, on page 145	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		command, you must be in a user group associated with a task group that includes appropriate task user group assignment is preventing you from using a command, contact your AAA administrator ice.
Note	All L2VPN	Configurations can be deleted using the no l2vpn command.
Task ID	Task Op ID	eration
	l2vpn rea wr	
	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
```

Related Commands	Command	Description	
	pw-class (L2VPN), on page 84	Enters pseudowire class submode to define a pseudowire class template.	
	pw-class encapsulation l2tpv3, on page 85	Configures L2TPv3 pseudowire encapsulation.	

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 config	uration submode	
Command History	Release	Modification	
	Release 3.7.2	This command was introduced.	
Usage Guidelines			oup associated with a task group that includes appropriate task you from using a command, contact your AAA administrator
Note	All L2VPN co	nfigurations can be deleted usin	g the no l2vpn command.
Task ID	Task Opera ID	tions	
	l2vpn read, write		
Examples	The following	example shows how to define a	simple pseudowire class template:
	RP/0/RSP0/CP RP/0/RSP0/CP RP/0/RSP0/CP RP/0/RSP0/CP	U0:router# configure U0:router(config)# 12vpn U0:router(config-12vpn)# x0 U0:router(config-12vpn-xc)# U0:router(config-12vpn-xc-p U0:router(config-12vpn-xc-p	p2p rtrA_to_rtrB (2p) # neighbor 10.1.1.2 pw-id 1000
Related Commands	Command	Descrij	tion
	p2p, on page S	•	2p configuration submode to configure point-to-point onnects.

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 $\{0 | 4 | 8\} | dfbit set | ipv4 source address | pmtu max 68-65535 | protocol l2tpv3 class name | sequencing both [{resync}]| tos {reflect value 0-255 | value 0-255 | transport-mode {ethernet vlan} | ttl value}]$

no pw-class class name encapsulation l2tpv3 [{cookie size $\{0 | 4 | 8\}$ | dfbit set | ipv4 source address | pmtu max 68-65535 | protocol l2tpv3 class name | sequencing both [{resync}] | tos {reflect value 0-255 | value 0-255 | transport-mode {ethernet vlan} | 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.		
	dfbit set	(Optional) Sets the Don't Fragment Bit (DFBIT)		
	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.		
	sequencing both	(Optional) Configures sequencing on both transmit and receive side		
	resync	(Optional) Sets the threshold for out-of-sequence packets before resync		
	transport-mode	(Optional) Configures the remote transport modeSets the transport mode as ethernet port modeSets the transport mode as vlan tagged mode(Optional) Configures TOS and the TOS value. Range is 0 to 255.		
	ethernet			
	vlan			
	tos { reflect value 0-255 value 0-255}			
	ttl value	Configures the Time-to-live (TTL) value. Range is 1 to 255.		
Command Default	None			
Command Modes	L2VPN pseudowire class configura	ation		
Command History	Release Modification			
	Release 3.9.0 This command was introduced.			
Usage Guidelines		in a user group associated with a task group that includes appropriate task s preventing you from using a command, contact your AAA administrator		
Note	All L2VPN configurations can be o	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:					
	<pre>RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# pw-class kanata01 RP/0/RSP0/CPU0:router(config-12vpn-pwc)# encapsulation 12tpv3 The following example shows how to set the encapsulation and protocol to L2TPV3:</pre>					
	RP/0/F RP/0/F RP/0/F	RSP0/CPU0:router# configure RSP0/CPU0:router(config)# 12vpn RSP0/CPU0:router(config-12vpn)# RSP0/CPU0:router(config-12vpn-pv RSP0/CPU0:router(config-12vpn-pv	vc)# encapsulation 12tpv3			
Related Commands	Comm	and	Description			
	pw-cl	ass (L2VPN), on page 84	Enters pseudowire class submode to define a pseudowire class template.			
	pw-cl	ass encapsulation mpls, on page 87	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 | redundancy one-way | sequencing | switching tlv | tag-rewrite | transport-mode | vccv verification-type none}

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

Syntax Description	class-name	Encapsulation class name.
	control word	Disables control word for MPLS encapsulation. Disabled by default.
	ipv4	Sets the local source IPv4 address.
	load-balancing	Sets flow label-based load balancing.

	preferred-pa	ath	Configures the preferred path tunnel settings.	
	protocol ldp		Configures LDP as the signaling protocol for this pseudowire class.	
	redundancy	one-way	Configures one-way PW redundancy behavior in the Redundancy Group.	
	sequencing		Configures sequencing on receive or transmit. Configures switching TLV to be hidden or not.	
	switching th	Ŷ		
	tag-rewrite		Configures VLAN tag rewrite.	
	transport-m	ode	Configures transport mode to be either Ethernet or VLAN. Enables or disables the VCCV verification type.	
	vccv none			
Command Default	None			
Command Modes	L2VPN pseud	lowire class configuration		
Command History	Release	Modification		
	Release 3.7.2	2 This command was introduced.		
	Release 3.9.0	The following keywords were added:		
		 preferred-path sequencing switching tlv tag-rewrite 		
	• transport-mode			
	Release 4.2.0	The keyword redundancy one-way was introduced.		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes approp IDs. If the user group assignment is preventing you from using a command, contact your AAA adm for assistance.			

Task ID	Task ID	Operations				
	l2vpn	read, write				
Examples	This example shows how to define MPLS pseudowire encapsulation:					
	RP/0/R RP/0/R	SP0/CPU0:ro SP0/CPU0:ro	r# configure r(config)# 12vpn r(config-12vpn)# pw-class kanata01 r(config-12vpn-pwc)# encapsulation mpls			
Related Commands	Comm	and	Description			
	pw-cla	ass (L2VPN), c	age 84 Enters pseudowire class submode to define a pseudowire class template.			

pw-ether

I

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 value Value of the PWHE Ethernet interface. The range is from 1 to 32768.						
					None	None
-						
Release	Modification	_				
Release 4.2.1	This command was introduced.	_				
IDs. If the use	r group assignment is preventi					
Task ID		Ор	eration			
interface (glo	bal configuration)	rea	d, write			
l2vpn (p2p co	onfiguration)	rea	d, write			
	no pw-ether value Value None Global config p2p configura Release Release 4.2.1 To use this con IDs. If the use for assistance. Task ID interface (glo	no pw-ether value value Value of the PWHE Ethernet interfa None Global configuration global configuration P2p configuration Release Modification Release 4.2.1 This command was introduced. To use this command, you must be in a user JDs. If the user group assignment is preventifor assistance.	no pw-ether value value Value of the PWHE Ethernet interface. The range is from 1 to 32768 None Global configuration g2p configuration P2p configuration Release Modification Release 4.2.1 This command was introduced. To use this command, you must be in a user group associated with a task group assignment is preventing you from using a command, for assistance. Task ID Op interface (global configuration) read			

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)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# xconnect group xc1
RP/0/RSP0/CPU0:router(config-12vpn-xc)#p2p grp1
RP/0/RSP0/CPU0:router(config-12vpn-xc-p2p)#interface pw-ether 78
```

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface pw-ether 78
RP/0/RSP0/CPU0:router(config-if)# 120verhead 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 92	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 configu	ration 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 Operation

 ID
 12vpn
 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)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# pw-grouping
```

Related Commands	Command	Description		
	l2vpn, on page 69	Enters L2VPN configuration mode.		
	show l2vpn, on page 108	Displays L2VPN information		

p2p

				figure point-to-point cross-connects, use the p2p command in fault behavior, use the no form of this command.		
	p2p xconnect-name no p2p xconnect-name					
Syntax Description	xconn	ect-name (O	ptional) Configures the	name of the point-to-point cross- connect.		
Command Default	None					
Command Modes	L2VPN	V xconnect				
Command History	Releas	se Mod	ification			
	Releas	se 3.7.2 This	command was introduce	ed.		
Usage Guidelines		the user grou		group associated with a task group that includes appropriate tas ing you from using a command, contact your AAA administrate		
	The na	me of the poi	nt-to-point cross-conne	ct string is a free format description string.		
Task ID	Task ID	Operations				
	l2vpn	read, write				
Examples		llowing examuration):	ple shows a point-to-po	oint cross-connect configuration (including pseudowire		
	RP/0/R RP/0/R	.SP0/CPU0:ro .SP0/CPU0:ro	outer# configure outer(config)# 12vpn outer(config-12vpn)# outer(config-12vpn-x	xconnect group group 1		
Related Commands	Comm	and		Description		
	interfa	ce (p2p), on	bage 58	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	•	v4 address : nn; where, IPv4 address is set to the BGP router-id lowire routing only, and nn is the index value that is					
Command Modes	L2VPN pseudowire routing BGP configuration submode						
	L2VPN bridge domain VFI autodiscovery BGP submode						
	L2VPN cross-connect mp2mp autodiscovery B	GP 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.					

	Release	Modification
	Release 5.3.1	For the L2VPN bridge domain VFI autodiscovery BGP and L2VPN cross-connect mp2mp autodiscovery BGP submodes, the index value associated with the IP address can take values higher than 32767 in the range from 0 to 65535.
		6
Usage Guidelines		p associated with a task group that includes appropriate task
Usage Guidelines Task ID	IDs. If the user group assignment is preventing y	p associated with a task group that includes appropriate task ou from using a command, contact your AAA administrator

```
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	2 This command was introduced.	
Usage Guidelines		er group assignment is prev	ser group associated with a task group that includes appropriate task renting you from using a command, contact your AAA administrator
		ure sequence resynch on h to 20 seconds of traffic.	igh speed circuits. On low speed circuits, do not configure a threshold
	<u> </u>		
Not	e This comman	d is not supported on the C	Cisco ASR 9000 Series Aggregation Services Router.
Not	e All L2VPN c	onfigurations can be delete	d using the no l2vpn command.
Task ID	Task Opera ID	tions	
	l2vpn read, write		
Examples	The following	g example shows how to co	onfigure L2VPN pseudowire class sequencing:
	RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C		-
Related Commands	Command		Description
	pw-class (L2	VPN), on page 84	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*}}

I

Syntax Description	bridge-do bridge-don		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 addre	ess:nn	Specifies the IPv4 address of the route distinguisher.		
			nn: 16-bit number		
	4-byte as-r	umber: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>:		
	2-byte as-number:nn		nn: 32-bit number 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	l was introduced.		
Usage Guidelines		iser group assignr	ust be in a user group associated with a task group that includes appropriate task nent is preventing you from using a command, contact your AAA administrator		
Task ID	– Task Op ID	eration			
	bgp rea	ıd			
	Example				
	-	e output shows the	e BGP routes associated with EVPN with bridge-domain filter:		

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

```
        show bgp
        l2vpn
        evpn
        bridge-domain
        bdl

        Network
        Next Hop
        Metric LocPrf Weight Path

        Route Distinguisher:
        192.0.2.1:1 (default for vrf bdl)

        *>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][0001.000	00.0001][0]/104				
*>	209.165.201.1		0	101	i
*>i[2][0][48][0002.000	0.0001][0]/104				
	203.0.113.1	100	0	102	i
* i	209.165.200.225	100	0	102	i
*>i[3][0][32][203.0.11	3.1]/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

show bgp l2vpn mspw

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

Syntax Description	This comma	nd 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		ser group assignment is preventing	oup associated with a task group that includes appropriate task you from using a command, contact your AAA administrator
Task ID	Task Ope ID	eration	
	bgp read	d	
	The followir	ng example displays the information	on 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, 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
```

show bgp vrf-db

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

	<pre>show bgp vfr-db{all vrf table id}</pre>			
Syntax Description	all	Displays all BGP VRF database table	e information.	
	vrf table id	Displays the BGP VRF database infor	rmation 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		er group assignment is preventing you	ssociated with a task group that includes appropriate tasl from using a command, contact your AAA administrato	
Task ID	Task Ope ID	ration		
	l2vpn read			
	Example			
	This sample	output shows the BGP VRF database i	nformation with the VRF table ID filter:	
		rf-db table 0x00000001 14:39:32.468 EDT		
		1 (L2VPN EVPN) x00000001 e: 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 detail

show evpn evi ead

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

	•	
Syntax Description	evi Specifies the EVPN Instance Identifier. This is used to derive the default Route Dist Route Targets.	tinguisher and
	ead Specifies the EVPN ead routes.	
	detail Displays detailed information.	
Command Default	None.	
Command Modes	EXEC	
Command History	Release Modification	
	ReleaseThis command was6.0.0introduced.	
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes a IDs. If the user group assignment is preventing you from using a command, contact your AAA for assistance.	
Task ID	Task Operation ID	
	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 00al.a2a3.a4a5.a6a7.a8a9 0 :: 2.2.2.2	24006 24007
	Source: Local, Remote, MPLS, VXLAN 1 00a1.a2a3.a4a5.a6a7.a8a9 ffffffff 2.2.2.2 Source: Remote, Unknown encap	0

	0000.0000.0000.0000.0000 1 urce: Local, MPLS	::	24025
200	0000.0000.0000.0000.0000 4 arce: Local, MPLS	::	24026
200	0000.0000.0000.0000.0000 11 arce: Local, MPLS	::	24027
	00a1.a2a3.a4a5.a6a7.a8a9 0	:: 2.2.2.2	24004 24005
Soi	arce: Local, Remote, MPLS, VXLA		21000
300	00a1.a2a3.a4a5.a6a7.a8a9 fffff	fff 2.2.2.2	0
Soi	ırce: Remote, Unknown encap		
302	00a1.a2a3.a4a5.a6a7.a8a9 0	::	24008
Soi	irce: Local, MPLS, VXLAN		
400	00b1.b2b3.b4b5.b6b7.b8b9 0	::	24010
Sou	arce: Local, MPLS		

Related Commands	Command	Description
evpn, on page 289		Enters EVPN configuration mode.
	evi, on page 288	Enters the EVPN EVI configuration mode to configure optional BGP settings for a bridge domain or EVI.

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		user group assignment is preventing	oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrato
Task ID	Task Op ID	peration	
	l2vpn rea	ad	

Example

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

<pre>show evpn internal-label vpn-id 1 detail Tue Jun 14 16:18:51.563 EDT</pre>					
EVI	Ethernet	Segment Id	EtherTag	Label	
Mul	lti-paths Lti-paths chlists:	00.0000.0000.0001 s resolved: TRUE s local label: 24036 1 entries	0	24036	
	, -	203.0.113.1 209.165.200.225		0 0	
	,	203.0.113.1 209.165.200.225		24001 24001	
	Summary	203.0.113.1 209.165.200.225		24001 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-confi	guration-pools	Displays auto configuration pool parameters.		
	dci-vrf-db		Displays DCI V	RF database information.	
	vrf vrf name		Displays DCI V	RF database for a specific VRF.	
	fabric fabr	ric id	Displays fabric information for fabric ID. The range is from 1000 to 9999. Displays opflex session information.		
	opflex-sess	sion			
	fabric-vrf-db		Displays fabric VRF database information.		
	fabric fabr	ric id	Displays fabric	/RF database for a fabric ID.	
Command Default	None				
Command Modes	EXEC				
Command History	Release	Modification			
	Release 6.1.2	This comman	d was introduced.		

Usage Guidelines To use this comma

To use this command, you must be in a user group associated with a task group that includes appropriate 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:

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:

Example

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

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.

I

	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				
	ReleaseThis command was introduced.4.3.0				
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate ta IDs. If the user group assignment is preventing you from using a command, contact your AAA administrat for assistance.				
Task ID	Task Operation ID				
	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:				
	<pre>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</pre>				

Related Commands	Command	Description	
	l2vpn, on page 69	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	(Optional) Displays attachment circuit information for a session.						
	detail	(Optional	(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	Configure	es the local tunnel	D. Range i	is 0 to 4294967295.	_			
	name name	Configure	es the tunnel name.			-			
Command Default	None								
Command Modes	EXEC								
Command History	Release	Modificati	on						
	Release 6.1.2	This comm	and was introduced	 I.					
Usage Guidelines		r group assi			ciated with a task group that in n using a command, contact y				
Task ID	Task Opera ID	ntions							
	l2vpn read, write								
Examples	The following	sample out	put is from the sh o	w l2tp ses	sion brief command:				
		CPU0:router(config-l2vpn-pw)# show l2tp session brief 12:51:30.901 UTC							
	LocID 1	'unID	Peer-address	State	Username, Intf/sess/cir	Vcid, Circuit			
			26.26.26.26 26.26.26.26	est,UP est,UP	101, Gi0/2/0/1.101 100, Gi0/2/0/1.100				

This table describes the significant fields shown in the display.

Table 1: show I2tp session brief Field Descriptions

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

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

```
RP/0/RP00/CPU0:router(config-12vpn-pw)# show 12tp 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 104

show l2tp tunnel

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

I

Syntax Description	detail	Displays det	ailed output for L 2TP tunnels			
			Displays detailed output for L2TP tunnels.			
	brief	1.	nmary information for the tunnel.			
	state	Displays con	trol plane state information.			
	transport	Displays tran	sport information (IP) for each selected control	ol channel.		
	id identifier	Displays loca	al control channel identifiers.			
	name local-nan	ne remote-name Displays the	local and remote names of a control channel.			
Command Default	None					
Command Modes	EXEC					
Command History	Release N	lodification				
	Release T 6.1.2	his command was introduced.				
Usage Guidelines			roup associated with a task group that includes g you from using a command, contact your A			
Task ID	Task Operatio	ons				
	l2vpn read, write					
Examples	The following sa	ample output is from the shov	v 12tp tunnel brief command:			
			ap-mpls)# show 12tp tunnel brief			
	Tue Jun 10 12: LocTunID Rem		ce Vrf Name Remote Address Sessn L2	2TP Class/Count		
	VPDN Group 1487464659 206	54960537 ASR9K-PE2 es	t 26.26.26.26 2	L2TPV3_CLASS		
	This table descri	bes the significant fields show	vn in the display.			
	Table 2: show l2tp tu	nnel Field Descriptions				
	Field	Description				
	LocTunID	Local session ID.				
	RemTunID	Remote session ID.	_			
	Remote Name	Remote name of the session	 I.			
	L	I				

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

Field	Description
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 I2tp session, on page 105	Displays information about L2TP sessions.

show I2vpn

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

show l2vpn

Syntax Description This command has no keywords or arguments.

L

Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 4.3.0	This command was introduced.	
Usage Guidelines		iser group assignment is preventin	oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task Op ID	eration	
	l2vpn rea	ad	

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 12vpn
Mon May 7 15:01:17.963 BST
PW-Status: disabled
 PW-Grouping: disabled
 Logging PW: disabled
Logging BD state changes: disabled
Logging VFI state changes: disabled
 Logging NSR state changes: disabled
 TCN propagation: disabled
 PWOAMRefreshTX: 30s
```

This 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 12vpn
Tue Oct 16 14:34:36.116 BST
PW-Status: enabled
PW-Grouping: disabled
Logging PW: disabled
Logging BD state changes: disabled
Logging VFI state changes: disabled
Logging NSR state changes: disabled
TCN propagation: disabled
PW OAM transmit time: 30s
Multicast P2MP: enabled
```

Related Commands	Command	Description		
	l2vpn, on page 69	Enters L2VPN configuration mode.		

Command	Description
pw-grouping, on page 91	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 M	odification
		his command was troduced.
Usage Guidelines		and, you must be in a user group associated with a task group that includes appropriate task oup assignment is preventing you from using a command, contact your AAA administrator
Task ID	Task Operations	
	l2vpn read	-
Examples	This example sho	ws the sample output of the show l2vpn atom-db source 1.1.1.1 command:
	RP/0/RSP0/CPU0:	router# show 12vpn atom-db source 1.1.1.1

I

	ource 1.1.1	VC ID 1	Encap MPLS	Signaling LDP	FEC 128	Discovery none	
This example shows the sample output of the show l2vpn atom-db source 1.1.1.1 detail command:							
RP/0/RSP0/CPU0:rou PW: neighbor 2.2 PW class class Encapsulation Source address PW type Etherr PW backup disa Sequencing not	hter# show 1 2.2.2, PW II 51, XC ID 05 MPLS, proto 5 1.1.1.1 het, control bble delay (L2vpn atom- D 1, state A DCOl LDP L word disa	- db source is down (1.1.1.1 deta provisioned	ail)		
	Local			Remote			
Label Group ID Interface MTU Control word PW type VCCV CV type	16000 0x20000060 GigabitEth 1504 disabled Ethernet e 0x2) nernet0/0/(0/1.1	unknown 0x0 unknown unknown unknown 0x0 (none)			
VCCV CC type	e Ox6	verificati lert label)		0x0 (none)			
Provisione Static tag n MTU: 1504 Tunnel inten IW type: 0 PW type: Dyn Pref path co Bridge port: BP learning BP ucast flo CW is mandat Label: local L2 Router-II LDP Router-J GR stale: No	3/12/2010 1 cus changed: info: .ass1 2.2.2, pseu l is not set d (Static) F ed Encapsula rewrite: not cface: None mamic onfigured: N ooding disabled: N ooding disabled: N ooding disabled: N ooding disable cory: No . unassigned cory: No . unassigned cory: 0.0.0.0 co. 0.0.0.0	15:28:26 (2 13/12/201 adowire ID Encapsulati ation: MPLS t set No bled: No bled: No d, remote u	10 15:28:20 = 1 ion: not se	5 (20:32:27 a	ado)		
LDP tag rewrit Force switchov MAC trigger: i VC sane: Yes Use PW Status: Local PW Statu Peer FEC Faile LSP: Down Operational st	<pre>te: not set ver: inactive nactive No us: Up(0x0); ed: No</pre>	7e					

I

	t: No : Yes o LDP: No rom LSD: Yes oy bit: No inding: No ening on : No			
	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 Reg 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		0x5e0		
12/13/2010 15:28:26				

show I2vpn collaborators

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

	show 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 incl IDs. If the user group assignment is preventing you from using a command, contact you for assistance.	
Task ID	Task Operations ID	
	l2vpn read, write	

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

RP/0/RSP0/CPU0:router	# show 12vpn	collaborator	s
L2VPN Collaborator st	ats:		
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 I2vpn 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.
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 47	Clears the state change counters for L2VPN collaborators.

show I2vpn database

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

	show l2vpn database {ac node}		
Syntax Description	ac Di	splays L2VPN Attachment Circuit (AC) database	
	node Di	splays 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 12vpn database ac
    Bundle-Ether1.1:
          Other-Segment MTU: 0
          Other-Segment status flags: 0x0
          Signaled capability valid: No
          Signaled capability flags: 0x0
          Configured capability flags: 0x0
          XCID: 0xfffffff
          PSN Type: Undefined
         ETH data:
              Xconnect tags: 0
              Vlan rewrite tag: 0
        AC defn:
            ac-ifname: Bundle-Ether1.1
            capabilities: 0x00368079
            extra-capabilities: 0x0000000
            parent-ifh: 0x020000e0
            ac-type: 0x15
            interworking: 0x00
        AC info:
            seg-status-flags: 0x0000000
            segment mtu/12-mtu: 1504/1518
    GigabitEthernet0/0/0/0.4096:
          Other-Segment MTU: 0
          Other-Segment status flags: 0x0
          Signaled capability valid: No
          Signaled capability flags: 0x0
          Configured capability flags: 0x0
          XCID: 0x0
          PSN Type: Undefined
         ETH data:
              Xconnect tags: 0
              Vlan rewrite tag: 0
        AC defn:
            ac-ifname: GigabitEthernet0 0 0 0.4096
            capabilities: 0x00368079
            extra-capabilities: 0x0000000
            parent-ifh: 0x040000c0
            ac-type: 0x15
            interworking: 0x00
        AC info:
            seg-status-flags: 0x0000003
            segment mtu/12-mtu: 1504/1518
```

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

MA: vlan ma

AC event trace history [Total events: 4]

Time		Event	Num Rcvd	Num Sent
		=====		
07/27/2012 1	5:00:31	Process joined	0	0
07/27/2012 1	5:00:31	Process init success	0	0
07/27/2012 1	5:00:31	Replay start rcvd	0	0
07/27/2012 1	5:00:31	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	s 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	e 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-domai	n Displays bridge domair	related forwarding	information.
	xconnect	Displays VPWS edge i	nformation.	
	summary	Displays summary info	ormation.	
	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				l with a task group that includes appropriate task ng a command, contact your AAA administrator
Task ID	Task Operati ID	ons		
	l2vpn read, write			
Examples	The following filter:	examples display output fo	or the show l2vpn d i	iscovery command with bridge-domain
	RP/0/RSP0/CP	U0:router# show 12vpn d	iscovery bridge-	domain
		: VPLS, Connected Ns (8001 VPNs):		
	VPLS-ID: Local L2	up: bgl, bridge-domain (auto) 1:101 router id: 10.10.10.1 Remote NLRI (3 NLRIs):	0	, signaling protocol: LDP
		dr Remote Addr		
	10.10.10 10.10.10 10.10.10	.1020.20.20.20.1030.30.30.30.1040.40.40	20.20.20.20 30.30.30.30 40.40.40.40	03/13/2010 21:27:05 03/13/2010 21:27:05 03/13/2010 21:27:05
	The following	examples display output f	or the show l2vpn of	discovery summary command:
	Sun Mar 14 1	U0:router# show l2vpn d 5:13:31.240 EDT ed=yes, active=yes,		

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 VPN Num Local Edges=0, Num Remote Ed	
Related Commands	Command	Description
	show I2vpn bridge-domain (VPLS), on page 223	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.

 $\begin{array}{l} show \ 12vpn \ forwarding \ \{xconnect \ | \ bridge-domain \ | \ counter \ | \ debug \ | \ detail \ | \ dhcp \ binding \ | \ ethernet \ ring \ g8032 \ | \ gsp \ | \ hardware \ | \ inconsistent \ | \ interface \ | \ 12tp \ | \ 12tpv2 \ | \ location \ \ [node-id] \ | \ message \ | \ monitor-session \ | \ mstp \ | \ neighbor \ | \ object-queues \ | \ pbb \ | \ protection \ | \ pwgroup \ | \ resource \ | \ retry-list \ | \ summary \ | \ unresolved \ \} \end{array}$

Syntax Description		Disularia the anexe connect related
Syntax Description	xconnect	Displays the cross-connect related information.
	bridge-domain	Displays bridge domain related forwarding information.
	counter	Displays the cross-connect counters.
	debug	Displays debug information.
	detail	Displays detailed information from the layer2_fib manager.
	dhcp binding	Displays DHCP binding related forwarding information
	ethernet ring g8032	Displays Ethernet associated configuration information.
	gsp	Displays GSP related forwarding information.
	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.

	l2tpv2	Displays l2tpv2 related forwarding information.
	location node-id	Displays layer2_fib manager information for the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
	message	Displays messages exchanged with collaborators.
	monitor-session	Displays the match Monitor-session.
	mstp	Displays multi-spanning tree related forwarding information.
	neighbor	Displays the match neighbor IP address.
	object-queues	Displays object queues related information.
	pbb	Displays l2vpn provider backbone bridge information.
	protection	Displays protection associated interfaces related forwarding information.
	pwgroup	Displays PW-Group related forwarding information.
	resource	Displays resource availability information in the layer2_fib manager.
	retry-list	Displays retry list related information.
	summary	Displays summary information about cross-connects in the layer2_fib manager.
	unresolved	Displays unresolved entries only.
Command Default	None	
command Modes	EXEC	

I

Command History	Release	Modification
	Release 3.7.2	This command was introduced.
	Release 4.3.0	The following keywords were introduced:
		• debug
		dhcp binding
		• ethernet ring g8032
		• gsp
		• l2tpv2
		monitor-session
		• neighbor
		• object-queues
		• pbb
		• protection
	Release 5.1	The pwgroup keyword was introduced.
	Release 5.3.1	The show command output was enhanced to display VXLAN anycast gateway parameters.
	Release 5.3.2	The show command output is enhanced to display MAC Move Counters information.
	Release 6.1.2	The show command output is enhanced to display the Service Path Preference parameters.
Usage Guidelines	appropriate tas	nds of this module, you must be in a user group associated with a task group that includes sk IDs. If the user group assignment is preventing you from using any command, contact your rator for assistance.
Task ID	Task Opera ID	tions
	l2vpn read	
Examples	-	sample output is from the show l2vpn forwarding bridge detail location command leases 5.3.1 and earlier:
	Bridge-domai MAC learnin Flooding: Broadcast Unknown u MAC aging t	& Multicast: enabled nicast: enabled ime: 300 s, Type: inactivity 4000, Action: none, Notification: syslog eached: no

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 12vpn forwarding bridge detail location 0/0/CPU0
```

```
Bridge-domain name: pbb:pbb core1, id: 10, state: up
Type: pbb-core
Number of associated pbb-edge BDs: 1
MAC learning: enabled
MAC port down flush: enabled
Flooding:
  Broadcast & Multicast: enabled
  Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC Secure: disabled, Logging: disabled
DHCPv4 snooping: profile not known on this node
 Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
IGMP snooping: disabled, flooding: enabled
MLD snooping: disabled, flooding: disabled
MMRP Flood Optimization: disabled
 Storm control: disabled
P2MP PW: disabled
Bridge MTU: 1500 bytes
Number of bridge ports: 1
Number of MAC addresses: 5
Multi-spanning tree instance: 0
PBB-EVPN: enabled
Statistics:
  packets: received 0, sent 963770
  bytes: received 0, sent 263433178
  PBB Core, state: Up
   Vlan-id: 1
   XC ID: 0x80000010
   Number of MAC: 0
   Statistics:
     packets: received 0 (unicast 0), sent 0
     bytes: received 0 (unicast 0), sent 0
     MAC move: 0
    Storm control drop counters:
     packets: broadcast 0, multicast 0, unknown unicast 0
     bytes: broadcast 0, multicast 0, unknown unicast 0
```

The following sample outputs shows the backup pseudowire information:

```
RP/0/RSP0/CPU0:router#show 12vpn 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 12vpn forwarding bridge-domain detail location 0/2/CPU0
Bridge-domain name: bg1:bd1, id: 0, state: up
.....
  GigabitEthernet0/2/0/0.4, state: oper up
   RG-ID 1, active
   Number of MAC: 0
   .....
  Nbor 101.101.101.101 pw-id 5000
   Backup Nbor 101.101.101.101 pw-id 5000
   Number of MAC: 0
RP/0/RSP0/CPU0:router#show 12vpn forwarding bridge-domain detail location 0/2/CPU0
Bridge-domain name: bg1:bd1, id: 0, state: up
GigabitEthernet0/2/0/0.4, state: oper up
XC ID: 0x1880002
Number of MAC: 0
Statistics:
packets: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent 963770
bytes: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent 263433178
MAC move: 0
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
```

```
... .
```

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

```
pw-span-test(monitor-session) mpls 2.2.2.2
                                                      IIP
pw-span-sess(monitor-session) mpls 3.3.3.3
                                                        UP
RP/0/RSP0/CPU0:router #Show 12vpn forwarding monitor-session pw-span-test location 0/7/CPU0
                               Segment 2
Segment 1
                                                                 State
  _____
pw-span-test(Monitor-Session) mpls 2.2.2.2
                                                     UP
Example 4:
RP/0/RSP0/CPU0:router #show 12vpn forwarding detail location 0/7/CPU0
 Xconnect id: 0xc000001, Status: up
 Segment 1
   Monitor-Session, pw-span-test, status: Bound
 Segment 2
   MPLS, Destination address: 2.2.2.2, pw-id: 1, status: Bound
   Pseudowire label: 16001
   Statistics:
    packets: received 0, sent 11799730
    bytes: received 0, sent 707983800
Example 5:
show 12vpn forwarding private location 0/11/CPU0
 Xconnect ID 0xc000001
 Xconnect info:
  Base info: version=0xaabbcc13, flags=0x0, type=2, reserved=0
  xcon bound=TRUE, switching type=0, data type=3
 AC info:
  Base info: version=0xaabbcc11, flags=0x0, type=3, reserved=0
   xcon id=0xc000001, ifh= none, subifh= none, ac id=0, ac type=SPAN,
   ac mtu=1500, iw mode=none, adj valid=FALSE, adj addr none
 PW info:
  Base info: version=0xaabbcc12, flags=0x0, type=4, reserved=0
   pw id=1, nh valid=TRUE, sig cap flags=0x20, context=0x0,
   MPLS, pw_label=16001
   Statistics:
    packets: received 0, sent 11799730
    bytes: received 0, sent 707983800
  Object: NHOP
  Event Trace History [Total events: 5]
_____
                                    Flags
   Time
                   Event
   ====
                    ____
                                    ____
 _____
 Nexthop info:
  Base info: version=0xaabbcc14, flags=0x10000, type=5, reserved=0
  nh addr=2.2.2.2, plat data valid=TRUE, plat data len=128, child count=1
  Object: XCON
  Event Trace History [Total events: 16]
_____
   Time
                  Event
                                    Flags
    ____
                    ____
                                     ____
 _____
```

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

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

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

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

The following sample output shows the MAC information in the layer2 fib manager summary:

RP/0/RSP0/CPU0:router# show 12vpn forwarding summary location 0/3/CPU0

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

This example shows sample output for the **show l2vpn forwarding location** command:

RP/0/RSP0/CPU0:router#	how 12vpn forwarding location 0/1/CPU0	
LC/0/1/CPU0:JSegment 1	Segment 2	State
PBB Edge	Bridge id 0, SHG id 0	UP
Gi0/1/0/1.1(Eth VLAN)	Bridge id 0, SHG id 0	UP
Gi0/1/0/1.2(Eth VLAN)	Bridge id 0, SHG id 0	UP
mpls 1.2.3.4,22	Bridge id 1, SHG id 0	DN
PBB Core	Bridge id 2, SHG id 0	UP

This example shows sample output for the **show l2vpn forwarding summary location** command:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding summary location 0/0/CPU0
Major version num:1, minor version num:0
Shared memory timestamp:0x4005e57a0
Number of forwarding xconnect entries:4
Up:4 Down:0
AC-PW:0 AC-AC:0 AC-BP:0 AC-Unknown:0
PW-BP:0 PW-Unknown:0
```

```
PBB-BP:4 PBB-Unknown:0
Number of xconnects down due to:
AIB:0 L2VPN:0 L3FIB:0
Number of p2p xconnects: 0
Number of bridge-port xconnects: 4
Number of nexthops:0
Number of bridge-domains: 5
Number of static macs: 0
Number of locally learned macs: 0
Number of remotely learned macs: 0
Number of total macs: 0
```

This example shows sample output for the **show l2vpn forwarding detail location** command for IOS-XR 5.3.1 and earlier releases:

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding detail location 0/1/CPU0
Local interface: TenGigE0/0/0/1/0.1, Xconnect id: 0x80005, Status: up
  Segment 1
   AC, TenGigE0/0/0/1/0.1, status: Bound
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
  Segment 2
    Bridge id: 19, Split horizon group id: 0
    Storm control: disabled
   MAC learning: enabled
   MAC port down flush: enabled
   Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
   MAC aging time: 300 s, Type: inactivity
   MAC limit: 4000, Action: none, Notification: syslog
   MAC limit reached: no
   MAC Secure: disabled, Logging: disabled, Accept-Shutdown: enabled
    DHCPv4 snooping: profile not known on this node, disabled
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    IGMP snooping profile: profile not known on this node
   MLD snooping profile: profile not known on this node
    Router guard disabled
    P2MP PW: disabled
Local interface: PBB Core, Xconnect id: 0x2000001, Status: up
  Segment 1
   AC, TenGigE0/0/0/1/0.1, status: Bound
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
  Segment 2
   Bridge id: 19, Split horizon group id: 0
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
```

This example shows sample output for the **show l2vpn forwarding detail location** command for IOS-XR 5.3.2 release

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding detail location 0/6/CPU0
Local interface: TenGigE0/0/0/1/0.1, Xconnect id: 0x80005, Status: up
Segment 1
    AC, TenGigE0/0/0/1/0.1, status: Bound
    Statistics:
        packets: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent 0
```

```
bytes: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent 0
   MAC move: 0
   packets dropped: PLU 0, tail 0
   bytes dropped: PLU 0, tail 0
Segment 2
 Bridge id: 19, Split horizon group id: 0
 Storm control: disabled
 MAC learning: enabled
 MAC port down flush: enabled
 Flooding:
   Broadcast & Multicast: enabled
   Unknown unicast: enabled
 MAC aging time: 300 s, Type: inactivity
 MAC limit: 4000, Action: none, Notification: syslog
 MAC limit reached: no
 MAC Secure: disabled, Logging: disabled, Accept-Shutdown: enabled
 DHCPv4 snooping: profile not known on this node, disabled
  Dynamic ARP Inspection: disabled, Logging: disabled
 IP Source Guard: disabled, Logging: disabled
 IGMP snooping profile: profile not known on this node
 MLD snooping profile: profile not known on this node
 Router guard disabled
  P2MP PW: disabled
```

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

RP/0/RSP0/CPU0:router# show 12vpn for location 0/0/CPU0

The following sample output is from the **show l2vpn forwarding neighbor ipv6** command:

RP/0/RSP0/CPU0:router# show l2vpn forwarding neighbor ipv6 1111:2222::cdef detail loc 0/0/cpu0

```
Fri May 18 13:58:14.720 EDT
Local interface: GigabitEthernet0/0/0/4.2, Xconnect id: 0x2, Status: up
Segment 1
AC, GigabitEthernet0/0/0/4.2, Ethernet VLAN mode, status: Bound
Statistics:
packets: received 0, sent 0
bytes: received 0, sent 0
Segment 2
L2TPv3-IPV6, Destination address: 1111:2222::cdef, status: Bound
Source address: 1111:2222::abcd
Local session:
Session ID: -1
Cookie: size 0 bytes
Remote session:
Session ID: -1
Cookie: size 0 bytes
Control word disabled
Sequencing not set
TOS 40 (reflect disabled), TTL 255, DF bit not set
Path MTU: disabled
Statistics:
packets: received 0, sent 0
```

bytes: received 0, sent 0 packets dropped: out of sequence 0, other 0

This example shows sample output for the **show l2vpn forwarding detail location** command with P2MP PW enabled on the PW BP for IOS-XR 5.3.1 and earlier releases.

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding detail location
Xconnect id: 0xfffc0003, Status: up
  Segment 1
   MPLS, Destination address: 2.2.2.2, pw-id: 101, status: Bound
   Pseudowire label: 16002 Control word disabled
    Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  Segment 2
    Bridge id: 0, Split horizon group id: 1
    Storm control: disabled
   MAC learning: enabled
   MAC port down flush: enabled
    Flooding:
     Broadcast & Multicast: enabled
     Unknown unicast: enabled
    MAC aging time: 300 s, Type: inactivity
   MAC limit: 4000, Action: none, Notification: syslog
   MAC limit reached: no
   MAC Secure: disabled, Logging: disabled
    DHCPv4 snooping: profile not known on this node, disabled
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    IGMP snooping profile: profile not known on this node
    Router guard disabled
    P2MP PW enabled
```

This example shows sample output for the **show l2vpn forwarding detail location** command with P2MP PW enabled on the PW BP for IOS-XR 5.3.2 release.

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding detail location
Xconnect id: 0xfffc0003, Status: up
  Segment 1
   MPLS, Destination address: 2.2.2.2, pw-id: 101, status: Bound
    Pseudowire label: 16002
                              Control word disabled
    Statistics:
        packets: received 1000 (unicast 1000), sent 0
        bytes: received 128000 (unicast 128000), sent 0
       MAC move: 10
  Segment 2
    Bridge id: 0, Split horizon group id: 1
    Storm control: disabled
   MAC learning: enabled
   MAC port down flush: enabled
   Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
   MAC aging time: 300 s, Type: inactivity
   MAC limit: 4000, Action: none, Notification: syslog
   MAC limit reached: no
   MAC Secure: disabled, Logging: disabled
    DHCPv4 snooping: profile not known on this node, disabled
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    IGMP snooping profile: profile not known on this node
    Router guard disabled
```

P2MP PW enabled

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

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding summary location
Mon Sep 9 22:07:54.000 EDT
Major version num:1, minor version num:0
Shared memory timestamp:0x547395c50
Global configuration:
Number of forwarding xconnect entries:5
 Up:0 Down:5
 AC-PW(atom):1 AC-PW(l2tpv2):0 AC-PW(l2tpv3):0
 (1 mpls) AC-AC:0 AC-BP:0 AC-Unknown:0
 PW-BP:4 PW-Unknown:0
 PBB-BP:0 PBB-Unknown:0
 Monitor-Session-PW:0 Monitor-Session-Unknown:0
Number of xconnects down due to:
 AIB:0 L2VPN:5 L3FIB:0 VPDN:0
Number of xconnect updates dropped due to:
 Invalid XID: 0 VPWS PW, 0 VPLS PW, 0 Virtual-AC, 0 PBB
 Exceeded max allowed: 0 VPLS PW, 0 Bundle-AC
Number of p2p xconnects: 1
Number of bridge-port xconnects: 4
Number of nexthops:2
 MPLS: Bound:2 Unbound:0 Pending Registration:0
 P2MP MLDP: Bound:1 Unbound:0 Pending Registration:0
 P2MP TE: Bound:1 Unbound:0 Pending Registration:0
Number of bridge-domains: 2 (0 with routed interface, 2 with P2MP enabled)
Number of bridge-domain updates dropped: 0
Number of static macs: 0
Number of routed macs: 0
Number of locally learned macs: 0
Number of remotely learned macs: 0
Number of total macs: 0
Number of total P2MP Ptree entries: 2
 MLDP:1 (LMRIB:1) RSVP-TE:0 (LMRIB:0)
```

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

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding detail location
Local interface: GigabitEthernet0/0/0/0.100, Xconnect id: 0x100009, Status: up
  Segment 1
   AC, GigabitEthernet0/0/0/0.100, Ethernet VLAN mode, status: Bound
    Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
  Segment 2
   MPLS, Destination address: 1.1.1.10, pw-id: 100, status: Bound, Active
    Pseudowire label: 16000 Control word disabled
   NHOP: 1.1.1.10, PW-Group Id: 0x1001
   Backup PW
     MPLS, Destination address: 3.3.3.30, pw-id: 300, status: Bound
     Pseudowire label: 16000
     NHOP: 3.3.3.30, Backup PW-Group Id: 0x1002
    Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
```

128

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

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding summary location 0/0/CPU0
Tue Jun 18 22:29:47.815 DST
Major version num:1, minor version num:0
Shared memory timestamp:0x182a49b4f9
Global configuration:
Number of forwarding xconnect entries:31
  Up:19 Down:12
 AC-PW(atom): 0 AC-PW(12tpv2): 0 AC-PW(12tpv3): 0
  AC-PW(12tpv3-ipv6):0
  AC-AC:3 AC-BP:16 AC-Unknown:0
 PW-BP:12 PW-Unknown:0
 PBB-BP:0 PBB-Unknown:0
 Monitor-Session-PW:0 Monitor-Session-Unknown:0
Number of xconnects down due to:
 AIB:0 L2VPN:12 L3FIB:0 VPDN:0
Number of xconnect updates dropped due to:
 Invalid XID: 0 VPWS PW, 0 VPLS PW, 0 Virtual-AC, 0 PBB
 Exceeded max allowed: 0 VPLS PW, 0 Bundle-AC
Number of p2p xconnects: 1
Number of PW-Group Ids: 1
Number of PW-Group Ids Down: 0
Number of bridge-port xconnects: 28
Number of nexthops:5
 MPLS: Bound:0 Unbound:5 Pending Registration:0
  P2MP MLDP: Bound:0 Unbound:0 Pending Registration:0
  P2MP TE: Bound:0 Unbound:0 Pending Registration:0
Number of bridge-domains: 14
 2 with routed interface
  0 with PBB evpn enabled
  0 with p2mp enabled
Number of bridge-domain updates dropped: 0
Number of total macs: 0
  0 Static macs
  0 Routed macs
  0 BMAC
  0 Source BMAC
  0 Locally learned macs
  0 Remotely learned macs
Number of total P2MP Ptree entries: 0
Number of EVPN Multicast Replication lists: 0 (0 default)
```

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

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

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

RP/0/RSP0/CPU0:router# show 12vpn forwarding pwgroup group-id 0x1001 loc 0/0/cpu0 Xconnect ID 0x1080001

```
PW info:
Base info: version=0xaabbcc12, flags=0x0, type=4, reserved=0
pw_id=100, nh_valid=TRUE, sig_cap_flags=0x20, context=0x0,
MPLS, Destination address: 1.1.1.10, pw-id: 100, status: Bound, Active
Pseudowire label: 16000 Control word disabled
Redundancy role: active, PW-Group Id 0x1001
Xconnect ID 0x1080008
PW info:
Base info: version=0xaabbcc12, flags=0x0, type=4, reserved=0
pw_id=108, nh_valid=TRUE, sig_cap_flags=0x20, context=0x0,
MPLS, Destination address: 1.1.1.10, pw-id: 108, status: Bound, Active
Pseudowire label: 16000 Control word disabled
Redundancy role none, FW-Group Id 0x1001
```

The example shows sample output for the **show l2vpn forwarding xconnect** command.

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding xconnect 0xfff8000f detail location 0/0/CPU0Mon
Jun 20 20:15:32.150 EDT
Xconnect id: 0xfff8000f, Status: up
Segment 1 MPLS, Destination address: 2.2.2.2, pw-id: 100:1001, status: Bound
Pseudowire label: 24055
Control word disabled
Forward-class: 1
Statistics:
    packets: received 0 (unicast 0), sent 0
    bytes: received 0 (unicast 0), sent 0
    MAC move: 0
Segment 2
Bridge id: 0, Split horizon group id: 1
Storm control: disabled
```

Related Commands	Command
------------------	---------

clear I2vpn forwarding counters, on page 49 Clears L2VPN forwarding counters.

show I2vpn forwarding message counters

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

Description

	<pre>show l2vpn forwarding message counters {hardware location node-id}</pre>		
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 Time	Count	Infol	Info2
==== l2vpn provision messages received:	0	0x0	0x0
-	0	0110	0110
12vpn unprovision messages received:	0	0x0	0x0
12vpn bridge provision messages received Jan 8 14:49:19.283	: 2	0x1	0x0
12vpn bridge unprovision messages receiv	ed: 0	0x0	0x0
- l2vpn bridge main port update messages r Jan 8 12:02:15.628	eceived: 1	0x2000300	0x0
12vpn bridge main port update w/ action=	MSTI_DELETE 0	0x0	0x0
- l2vpn bridge main port update ACK sent: Jan 8 12:02:15.628	1	0x2000300	0x0
12vpn bridge port provision messages rec Jan 8 12:02:15.629	eived: 1	0x2000002	0x0
12vpn bridge port unprovision messages r -	eceived: 0	0x0	0x0
12vpn shg provision messages received: -	0	0x0	0x0
12vpn shg unprovision messages received:	0	0x0	0x0
l2vpn static mac provision messages rece Jan 9 08:41:36.668	ived: 1	0x0	0x0
l2vpn static mac unprovision messages re Jan 9 08:44:24.208	ceived: 1	0x0	0x0
12vpn dynamic mac local learning message	s received: 0	0x0	0x0
- 12vpn dynamic mac remote learning messag -	es received O	0x0	0x0
12vpn dynamic mac refresh messages recei	ved: 0	0x0	0x0
12vpn dynamic mac unprovision messages r	eceived: 0	0x0	0x0

-			
AIB update messages received: Jan 8 12:02:15.622	4	0x2000102	0x2000300
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 I2vpn forwarding message counters, on page 51	Clears L2VPN forwarding message counters.

show I2vpn 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 in	nterface.	
	name	Specifies the name of the int	terface.	
	private	Specifies the private details	of the interface.	
	summary	Specifies the summary inform	nation of the interface.	
Command Default	None			
Command Modes	EXEC			
Command History	Release	Modification		
	Release 4.2	.1 This command was introduced.		
Usage Guidelines		ser group assignment is preve		th a task group that includes appropriate task command, contact your AAA administrator

Task ID	Task Operations ID		
	l2vpn read		
Examples	This example shows the sample output of the show l2vpn generic-interface-list command:		
	RP/0/RSP0/CPU0:router# show 12vpn generic-interface-list generic-interface-list: 11 (ID: 2, interfaces: 2) Number of items: 20 generic-interface-list: 12 (ID: 3, interfaces: 4) Number of items: 15		
	This example shows the sample output of the show l2vpn generic-interface-list detail command:		
	<pre>RP/0/RSP0/CPU0:router# show 12vpn generic-interface-list detail generic-interface-list: 11 (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</pre>		
	<pre>generic-interface-list: 12 (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</pre>		
	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 11 detail
generic-interface-list: l1 (ID: 2, interfaces: 2)
GigabitEthernet0/1/0/0 - items pending 2
GigabitEthernet0/1/0/1 - items pending 4
Number of items: 20
PW-Ether 1-10, 12-21
```

show l2vpn index

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

show l2vpn index [{location | private | standby}]

Syntax Description	location	(Optional) Displays index manager statistics for the specified location.
	private	(Optional) Detailed information about all indexes allocated for each pool.

	standby		(Optional) Displays Standby node specific information.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 4.2.1	This command was introduced.	
	Release	The following keywords are introduced:	
	4.3.0	location	
		• standby	
Usage Guidelines		iser group assignment is preventing you from	iated with a task group that includes appropriate task a using a command, contact your AAA administrator
Task ID	Task Ope ID	erations	
	l2vpn rea	d	
Examples	This examp	le shows the sample output of the show l2vp	on index command:
	Pool ic Pool si zombiec allocat Pool ic Pool si zombiec	<pre>/CPU0:router# show 12vpn index d: 0x4, App: RD ize: 32767 d IDs: 0 ced IDs: 0 d: 0x5, App: IFLIST ize: 65535 d IDs: 0</pre>	
	Pool ic Pool si zombiec	<pre>ted IDs: 2 d: 0xff000001, App: PW/PBB/Virtual AC lize: 40960 d IDs: 0 ted IDs: 1</pre>	
	Pool si zombiec	d: 0xff000002, App: BD Lze: 4095 d IDs: 0 ced IDs: 2	
	Pool si zombiec	d: 0xff0000003, App: MP2MP Lze: 65535 d IDs: 0 ced IDs: 1	

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

```
RP/0/RSP0/CPU0:router# show 12vpn index standby
   Pool id: 0xfffc0000, App: Global
      Max number of ID mgr instances: 1
      ID mgr instances in use: 1
      Pool size: 98304
      zombied IDs: 0
      allocated IDs: 0
    Pool id: 0xfffc0002, App: BD
      Max number of ID mgr instances: 1
      ID mgr instances in use: 1
      Pool size: 8192
      zombied IDs: 0
      allocated IDs: 0
    Pool id: 0xfffc0003, App: MP2MP
      Max number of ID mgr instances: 1
      ID mgr instances in use: 1
      Pool size: 65535
      zombied IDs: 0
      allocated IDs: 0
```

show 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.		
	Release 6.1.2	The show command output was updated.		
Usage Guidelines		user group assignment is preventing you from	iated with a task group that includes appropriate task a using a command, contact your AAA administrator	

Task ID Task Operation ID

l2vpn read

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

RP/0/RSP0/CPU0:router# show 12vpn 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 ΡW : 1 ВD : 0 MP2MP : 0 RD : 0 PBB : 0 IFLIST : 0 ATOM : 1 : 0 Global PWGroup : 0 EVPN : 0

Related Commands	Command	Description
	l2vpn, on page 69	Enters L2VPN configuration mode.
	#unique_113	

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.

To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** 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 12vpn process fsm

Mon May 16 10:20:30.967 PDT L2VPN Process FSM		
Current process role	: Primary Active (Master)	
Current process state	: Run	
S/w install in progress	: No	
NSR Status:		
NSR 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 : O	
	MP2MP : O	
	RD : O	
	PBB : O	
	IFLIST : O	
	ATOM : 1	
	Global : O	
	PWGroup : 0	
	EVPN : O	
Process Role Change Statu	s:	
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 Repo	rt Card:	
Collaborator Con	nection 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 69	Enters L2VPN configuration mode.
	#unique_113	
	show l2vpn index, on page 133	Displays statistics about the index manager.

show I2vpn provision queue

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

Syntax Description	location	(Optional) Displays L2VPN configuration provisioning queue information	for the specified
	location	location.	for the specified
	standby	(Optional) Displays Standby node specific information.	
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release	This command was introduced.	
	4.3.0		
Usage Guidelines	$-\frac{4.3.0}{\text{To use this}}$	s command, you must be in a user group associated with a task group that incle user group assignment is preventing you from using a command, contact you	
Usage Guidelines Task ID	4.3.0 To use this IDs. If the for assista	s command, you must be in a user group associated with a task group that incle user group assignment is preventing you from using a command, contact you	
	4.3.0 To use this IDs. If the for assista Task 0	s command, you must be in a user group associated with a task group that incle e user group assignment is preventing you from using a command, contact you ince.	
	4.3.0 To use this IDs. If the for assista Task 0 ID 12vpn re	s command, you must be in a user group associated with a task group that incle e user group assignment is preventing you from using a command, contact you ince.	r AAA administrato
	4.3.0 To use this IDs. If the for assista Task 0 ID 12vpn re The follow	s command, you must be in a user group associated with a task group that incle e user group assignment is preventing you from using a command, contact you ince.	r AAA administrato

BD_NAME VPLS01	bd_t	vpls_bd_class	0/0/0 BD
VELSUI			
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:

Configuration Item	Object Type	Class	P/P/R Object
Кеу			
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			0/0/0 55
BD_NAME	bd_t	vpls_bd_class	0/0/0 BD
VPLS04 BD NAME	bd t	vpls bd class	0/0/0 BD
VPLS05	bu_t	vpis_bu_ciass	0/0/0 80
BD NAME	bd t	vpls bd class	0/0/0 BD
VPLS06		1	-, -, -
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 VPLS010	bd_t	vpls_bd_class	0/0/0 BD

Related Commands Co	ommand
---------------------	--------

l2vpn, on page 69

...

show I2vpn pw-class

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

Description

Enters L2VPN configuration mode.

. .

show	l2vpn	pw-class	[{detail	location	name	class	name standby}]	
------	-------	----------	----------	----------	------	-------	------------------	--

. .

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

Command Default	None					
Command Modes	EXEC					
Command History	Release	Modification				
	Release 3.7.2	This command	was introduced.			
	Release 4.3.0	The keywords le	ocation and standby	were introduced.		
Usage Guidelines		r group assignme			sk group that includes appropriate task nand, contact your AAA administrator	
Task ID	Task Opera ID	ations				
	l2vpn read					
Examples	The following	The following example shows sample output for the show l2vpn pw-class command:				
	RP/0/RSP0/CI	RP/0/RSP0/CPU0:router# show 12vpn pw-class				
	Name		Encapsulation	Protocol		
	mplsclass_75 l2tp-dynamic	5	MPLS L2TPv3	LDP L2TPv3		
	This example shows sample output for the show l2vpn pw-class detail command:					
	Encapsu Transpor Sequenc Static t PW Backu MAC with	RP/0/RSP0/CPU0:router# show l2vpn pw-class detail Encapsulation MPLS, protocol LDP Transport mode not set, control word unset (default) Sequencing not set Static tag rewrite not set PW Backup disable delay: 0 sec MAC withdraw message is sent over PW: no IPv4 source address 1.1.1.1				
	This table describes the significant fields shown in the display.					
	Table 4: show l2vpn pw-class Command Field Descriptions					
	Field	Description				
		1				

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

VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers, IOS XR Release 6.4.x

Field	Description
Protocol	Displays the protocol type.

show l2vpn pwhe {detail | interface | summary}

Related Commands

Command

clear I2vpn forwarding counters, on page 49	Clears L2VPN forwarding counters.

Description

show l2vpn pwhe

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

Syntax Description detail Specifies the details of the interface. interface Specifies the name of the interface. summary Specifies the summary information of the interface. None **Command Default** EXEC **Command Modes Command History** Release Modification Release 4.2.1 This command was introduced. To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. Task ID Operations Task ID l2vpn read **Examples** This example show the sample output for **show l2vpn pwhe detail** command: RP/0/RSP0/CPU0:router# show 12vpn 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 I2vpn resource

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

	5110w 12vpi	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.	
Ilsane Guidelines	To use this cor	nmand, you must be in a user gro	

show 12vnn resource

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

Task ID	Task Operations ID	
	l2vpn read	
Examples	The following example shows sample output for the show l2vpn resource command	:
	RP/0/RSP0/CPU0:router# show 12vpn resource	
	Memory: Normal	
	describes the significant fields shown in the display. Table 5: show l2vpn resource Co Descriptions, on page 143	mmand Field
	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</n>
	location	Displays trace data for the specified location.
	reverse	Display latest traces first
	stats	Display trace statistics
	tailf	Display new traces as they are added
	unique	Display unique entries with counts
	usec	Display usec details with timestamp
	verbose	Display internal debugging information
	wide	Display trace data excluding buffer name, node name, tid

	wrapping Display wrapping entries				
Command Default	None				
Command Modes	EXEC				
Command History	Release Modification				
	Release This command was introduced. 4.3.0				
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.				
Task ID	Task Operation ID				
	12vpn read				
	This example displays output for the show l2vpn trace command:				
	<pre>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 read'.</pre>				
	<pre>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</pre>				
	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				
	<pre>= 4832 (real: True) Jul 27 14:39:55.351 l2vpn/fwd-mac 0/RSP0/CPU0 1# t1 FWD_MAC:626: Entering mac aging</pre>				

This example displays output with MIRP-Lite entries 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

timer init

```
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 12vpn/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
   Jul 27 14:39:55.361 l2vpn/fwd-common 0/RSP0/CPU0 t1 FWD COMMON:1522:
############MIRP LITE SPIO
   Jul 27 14:39:55.362 l2vpn/fwd-common 0/RSP0/CPU0 t1 FWD COMMON:1561: MIRP-lite init
finished
   Jul 27 14:39:55.362 l2vpn/fwd-common 0/RSP0/CPU0 t1 FWD COMMON:1563: MIRP-lite
```

show I2vpn 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 | location | mp2mp | mspw | neighbor | pw-class | pw-id | standby | state | summary | | pw-id value | 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.
	location	(Optional) Displays location specific information.
	mp2mp	(Optional) Displays MP2MP information.
	mspw	(Optional) Displays MSPW information.
	neighbor	(Optional) Filters on neighbor.
	pw-class	(Optional) Filters on pseudowire class
	standby	(Optional) Displays standby node specific information.

	state	(Optional) Filters the following xconnect state types:
		• up
		• down
		• unresolved
	summary	(Optional) Displays AC information from the AC Manager database.
	pw-id value	(Optional) Displays the filter for the pseudowire ID. The range is from 1 to 4294967295.
	type	(Optional) Filters the following xconnect types:
		• ac-pw
		locally switched
		monitor-session-pwms-pw
Command Default	None	
Command Modes	EXEC	
Command History	Release	Modification
	Release 3.7.2	This command was introduced.
	Release 4.3.0	The following keywords were introduced:
		• location
		• standby
	Release 5.1.2	This command was modified to enable filtering the command output for a specific pseudowire with just the pseudowire ID.
Usage Guidelines		nmand, you must be in a user group associated with a task group that includes appropriate tasl r group assignment is preventing you from using a command, contact your AAA administrato
	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.	
	Continuity Ch	ring Ethernet Connectivity Fault Managment (CFM) over l2vpn cross-connect, the CFM eck Messages (CCM) packets are not accounted for in the cross-connect pseudowire packet ayed in this show command output.
Note		XR software Release 5.1.2 and above, you can filter the command output for specific pseudowire seudowire ID. However, for pseudowire configurations with EEC 120 Type 2 (in VPWS)
		seudowire ID. However, for pseudowire configurations with FEC 129 Type 2 (in VPWS), atput for a specific pseudowire can only be done with the combination of the neighbour filter owire ID.

fask ID	Task ID	Operations						
	l2vpn	read, write						
camples	The fol	lowing examp	le shows	sample output for the s	how l2vpn xo	connect command:		
	Wed Ma	y 21 09:06:4 : ST = State	7.944 U , UP = 0	bw 12vpn xconnect IC Jp, DN = Down, AD = = Standby Ready, (PE				
		Name		Segment 1 Description				
		_V4_XC_GRP L2TPV3_	P2P 1	Gi0/2/0/1.2				
	L2TPV3	V4_XC_GRP L2TPV3	P2P 2					
	xcon	nect deta	il comm	ut shows that the ba and: ow 12vpn xconnect de		standby mode for	the sh	ow 121
	XCON RP/0/R: Group : Moni: AC: 0 Tyj MTI Sta Sta Sta Sta PW: 1 PW:	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not	il comm ter# sho siva_p2p pw-spar net0/4/(D 0x5000 s: send send 19 1.1.1, f et, XC 1 MPLS, pr et, cont ble dela	and: bw 12vpn xconnect de p, state is up; Inte n-test, state is cor 0/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec	etail erworking no figured none; MSTi 0 o (establis	ne hed) none	the sh	ow 12v
	XCON RP/0/R Group : Moni AC: 0 Typ MT St. St. J PW: 1 PW: 1 PW: 1 PW: 2 PW: 2	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not MPLS	<pre>il comm ter# sho siva_p2p pw-span net0/4/0 D 0x5000 s: send 19 1.1.1, h et, XC 1 MPLS, pp et, cont ble dela set Local</pre>	and: bw 12vpn xconnect de p, state is up; Inte n-test, state is cor D/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec	etail erworking no hfigured none; MSTi 0 o (establis .nterworking Remo	ne hed) none		ow 121
	XCON RP/0/R Group : Moni- AC: 0 Typ MTU Sta 1 PW: 1 PW: 1 PW: 1 PW: 2 PW End PW Sed	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not MPLS 	il comm ter# sho siva_p2p pw-span net0/4/0 D 0x5000 s: send 1.1.1, n et, XC 1 MPLS, pp et, cont ble dela set Local 	and: bw 12vpn xconnect de p, state is up; Inten- test, state is cor 0/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec 1	etail erworking no hfigured none; MSTi 0 o (establis .nterworking Remo	ne hed) none		ow 12x
	XCON RP/0/R Group : Moni- AC: 0 Typ MTU Sta 1 PW: 1 PW: 1 PW: 1 PW: 2 PW End PW Sed	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not MPLS Label Group ID Interface	<pre>il comm ter# sho siva_p2p pw-span net0/4/0 D 0x5000 s: send send 19 1.1.1, n et, XC 1 MPLS, pr et, cont ble dela set Local </pre>	and: bw 12vpn xconnect de p, state is up; Inten- test, state is cor 0/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec 1 300 tEthernet0/4/0/1	etail erworking no ofigured none; MSTi 0 o (establis .nterworking 	ne hed) none te 400 tEthernet0/4/0/2		ow 12x
	XCON RP/0/R3 Group : Moni- AC: (Tyr MTU Sta 1 PW: 1 PW: 1 PW: 2 PW Ena PW Sea	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not MPLS Label Group ID Interface Interface	<pre>il comm ter# sho siva_p2p pw-span net0/4/0 D 0x5000 s: send send 19 1.1.1, n et, XC 1 MPLS, pr et, cont ble dela set Local </pre>	and: bw 12vpn xconnect de p, state is up; Inten- test, state is cor 0/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec 1 300 tEthernet0/4/0/1	etail erworking no ofigured none; MSTi 0 o (establis .nterworking 	ne hed) none te 400		ow 12v
	XCON RP/0/R3 Group : Moni: AC: (Tyr MTV Sta 1 PW: 1 PW: 1 PW Enc PW Sec ((() () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () ()) ()) () ()) () ()) ()) ()) ()) ())) ())) ()) ())) ()) ()))) ())))))) ()))))))))))))	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not MPLS Label Group ID Interface Interface	<pre>il comm ter# sho siva_p2p pw-span net0/4/0 D 0x5000 s: send send 19 1.1.1, n et, XC 1 MPLS, pr et, cont ble dela set Local </pre>	and: bw 12vpn xconnect de p, state is up; Inten- test, state is cor 0/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec 1 300 tEthernet0/4/0/1 n-test	etail erworking no ofigured none; MSTi 0 o (establis .nterworking 	hed) none te 400 tEthernet0/4/0/2 thernet0/3/0/1		ow 12x
	XCON RP/0/R3 Group : Monir AC: (Tyr MTV Sta 1 PW: 1 PW: 1 PW: 2 PW Ena PW Sea () () ()))))))))))))	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not MPLS 	<pre>il comm ter# sha siva_p2p pw-span net0/4/(D 0x5000 s: send 19 1.1.1, 1 et, XC 3 MPLS, pp et, cont ble dela set Local 30005 0x50003 Gigabit pw-span 1500 enabled Etherned</pre>	and: bw 12vpn xconnect de p, state is up; Inten- test, state is cor 0/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec 1 300 tEthernet0/4/0/1 n-test d	etail erworking no figured none; MSTi 0 o (establis nterworking Remo 16003 0x5000 Gigabi GigabitE 1500 enable Ethern	ne hed) none te 400 tEthernet0/4/0/2 thernet0/3/0/1		ow 121
	XCON RP/0/R3 Group : Monir AC: (Tyr MTV Sta 1 PW: 1 PW: 1 PW: 2 PW Ena PW Sea () () ()))))))))))))	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not MPLS 	<pre>il comm ter# sha siva_p2p pw-span net0/4/0 D 0x5000 s: send 19 1.1.1, 1 et, XC 1 MPLS, pp et, cont ble dela set Local 30005 0x50003 Gigabit pw-span 1500 enabled Etherne 0x2</pre>	and: bw 12vpn xconnect de p, state is up; Inte n-test, state is cor 0/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec 1 	etail erworking no figured none; MSTi 0 o (establis nterworking Remo 16003 0x5000 Gigabit GigabitE 1500 enable Ethern 0x2	ne hed) none te 400 tEthernet0/4/0/2 thernet0/3/0/1 d et		ow 121
	XCON RP/0/RS Group : Moni: AC: (Tyr MTT Sta 1 PW: 1 PW: 1 PW: 2 PW Ena PW Sea 1 1 1 1 1 1 1 1 1 1 1 1 1	spo/CPU0:rou siva_xc, XC tor-Session: GigabitEther pe Ethernet U 1500; XC I atistics: packet total byte totals: neighbor 10. class not s capsulation type Ethern backup disa quencing not MPLS 	<pre>il comm ter# sha siva_p2p pw-span net0/4/(D 0x5000 s: send send 19 1.1.1, 1 et, XC 1 MPLS, pr et, cont ble dela set Local 30005 0x50003 Gigabit pw-span 1500 enabled Etherne 0x2 (LSP p:</pre>	and: bw 12vpn xconnect de p, state is up; Inten- test, state is cor 0/1, state is up 0001; interworking r 90 9056 PW ID 1, state is up ID 0x5000001 rotocol LDP trol word enabled, i ay 0 sec 1 300 tEthernet0/4/0/1 n-test d	etail erworking no figured none; MSTi 0 o (establis nterworking Remo 16003 0x5000 Gigabit GigabitE 1500 enable Ethern 0x2	ne hed) none te 400 tEthernet0/4/0/2 thernet0/3/0/1		ow 121

```
Last time status changed: 20/11/2007 21:45:11 (00:49:14 ago)
 Statistics:
   packet totals: receive 0
   byte totals: receive 0
Backup PW:
PW: neighbor 2.2.2.2, PW ID 2, state is up ( established )
 Backup for neighbor 1.1.1.1 PW ID 1 ( standby )
 PW class not set, XC ID 0x0
 Encapsulation MPLS, protocol LDP
 PW type Ethernet, control word enabled, interworking none
 PW backup disable delay 0 sec
 Sequencing not set
    MPLS
           Local
                                            Remote
   _____ ____
             30006
   Label
                                          16003
   Group ID
   Group ID unassigned
Interface unknown
MTU 1500
                                          0x5000400
                                          GigabitEthernet0/4/0/2
                                         1500
   Control word enabled
                                         enabled
   PW type Ethernet
                                         Ethernet
   VCCV CV type 0x2
                                         0x2
              (LSP ping verification)
                                         (LSP ping verification)
                                         0x3
   VCCV CC type 0x3
               (control word)
                                          (control word)
              (router alert label)
                                         (router alert label)
   _____ ____
 Backup PW for neighbor 10.1.1.1 PW ID 1
 Create time: 20/11/2007 21:45:45 (00:48:40 ago)
 Last time status changed: 20/11/2007 21:45:49 (00:48:36 ago)
 Statistics:
   packet totals: receive 0
   byte totals: receive 0
```

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

RP/0/RSP0/CPU0:router# show 12vpn xconnect detail

Group siva xc, XC siva p2p, state is down; Interworking none Monitor-Session: pw-span-test, state is configured AC: GigabitEthernet0/4/0/1, state is up Type Ethernet MTU 1500; XC ID 0x5000001; interworking none; MSTi 0 Statistics: packet totals: send 98 byte totals: send 20798 PW: neighbor 10.1.1.1, PW ID 1, state is down (local ready) PW class not set, XC ID 0x5000001 Encapsulation MPLS, protocol LDP PW type Ethernet, control word enabled, interworking none PW backup disable delay 0 sec Sequencing not set MPLS Local Remote _____ 30005 Label unknown Group ID 0x5000300 0×0 Interface GigabitEthernet0/4/0/1 unknown GigabitEthernet0/3/0/1 Interface pw-span-test мти 1500 unknown Control word enabled unknown PW type Ethernet unknown VCCV CV type 0x2 0x0 (none)

```
(LSP ping verification)
   VCCV CC type 0x3
                                          0x0
                                          (none)
               (control word)
              (router alert label)
 Create time: 20/11/2007 21:45:06 (00:53:31 ago)
 Last time status changed: 20/11/2007 22:38:14 (00:00:23 ago)
 Statistics:
   packet totals: receive 0
   byte totals: receive 0
Backup PW:
PW: neighbor 10.2.2.2, PW ID 2, state is up ( established )
 Backup for neighbor 10.1.1.1 PW ID 1 ( active )
 PW class not set, XC ID 0x0
 Encapsulation MPLS, protocol LDP
 PW type Ethernet, control word enabled, interworking none
 PW backup disable delay 0 sec
 Sequencing not set
   MPLS Local
                                           Remote
   _____
                                                  _____
   Label 30006
Group ID unassigned
                                          16003
                                         0x5000400
   Interface unknown
                                         GigabitEthernet0/4/0/2
   MTU
             1500
                                         1500
   Control word enabled
                                         enabled
   PW type Ethernet
                                         Ethernet
   VCCV CV type 0x2
              0x2
(LSP ping verification)
                                         0x2
                                         (LSP ping verification)
   VCCV CC type 0x3
                                        0x3
               (control word)
                                          (control word)
              (router alert label)
                                         (router alert label)
   _____ ____
 Backup PW for neighbor 10.1.1.1 PW ID 1
 Create time: 20/11/2007 21:45:44 (00:52:54 ago)
 Last time status changed: 20/11/2007 21:45:48 (00:52:49 ago)
 Statistics:
   packet totals: receive 0
   byte totals: receive 0
```

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

```
      Show 12vpn xconnect type minotor-session-pw

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

      XConnect
      Segment 1

      Group
      Name
      ST

      J
      X1
      UP

      up
      2.2.2.2
      1

      UP
      UP
      2.2.2.2
      1
```

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 12vpn xconnect

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

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

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

RP/0/RSP0/CPU0:router# show 12vpn xconnect detail

Group siva xc, XC siva p2p, state is up; Interworking none AC: GigabitEthernet0/4/0/1, state is up Type Ethernet MTU 1500; XC ID 0x5000001; interworking none; MSTi 0 Statistics: packet totals: received 90, sent 90 byte totals: received 19056, sent 19056 PW: neighbor 1.1.1.1, PW ID 1, state is up (established) PW class not set, XC ID 0x5000001 Encapsulation MPLS, protocol LDP PW type Ethernet, control word enabled, interworking none PW backup disable delay 0 sec Sequencing not set MPLS Local Remote _____ ------

```
Label
             30005
                                        16003
   Group ID 0x5000300
                                        0x5000400
   Interface GigabitEthernet0/4/0/1
                                       GigabitEthernet0/4/0/2
   MTU
             1500
                                        1500
   Control word enabled
                                        enabled
   PW type Ethernet
                                        Ethernet
   VCCV CV type 0x2
                                        0x2
              (LSP ping verification)
                                        (LSP ping verification)
   VCCV CC type 0x3
                                       0x3
              (control word)
                                         (control word)
              (router alert label)
                                        (router alert label)
   _____
                                 Create time: 20/11/2007 21:45:07 (00:49:18 ago)
 Last time status changed: 20/11/2007 21:45:11 (00:49:14 ago)
 Statistics:
   packet totals: received 0, sent 0
   byte totals: received 0, sent 0
Backup PW:
PW: neighbor 2.2.2.2, PW ID 2, state is up ( established )
 Backup for neighbor 1.1.1.1 PW ID 1 ( standby )
 PW class not set, XC ID 0x0
 Encapsulation MPLS, protocol LDP
 PW type Ethernet, control word enabled, interworking none
 PW backup disable delay 0 sec
 Sequencing not set
    MPLS Local
                                          Remote
   ----- -
                                         16003
   Label 30006
   Group ID unassigned
                                        0x5000400
   Interface unknown
                                        GigabitEthernet0/4/0/2
   MTU
             1500
                                        1500
                                        enabled
   Control word enabled
   PW type Ethernet
                                        Ethernet
   VCCV CV type 0x2
                                        0x2
              (LSP ping verification)
                                        (LSP ping verification)
   VCCV CC type 0x3
                                       0x3
              (control word)
                                        (control word)
              (router alert label)
                                        (router alert label)
   _____ ____
 Backup PW for neighbor 1.1.1.1 PW ID 1
 Create time: 20/11/2007 21:45:45 (00:48:40 ago)
 Last time status changed: 20/11/2007 21:45:49 (00:48:36 ago)
 Statistics:
   packet totals: received 0, sent 0
   byte totals: received 0, sent 0
```

The following sample output shows that the backup is active for the **show 12vpn xconnect detail** command:

RP/0/RSP0/CPU0:router# show 12vpn xconnect detail

Group siva_xc, XC siva_p2p, state is down; Interworking none AC: GigabitEthernet0/4/0/1, state is up Type Ethernet MTU 1500; XC ID 0x5000001; interworking none; MSTi 0 Statistics: packet totals: send 98 byte totals: send 20798 PW: neighbor 1.1.1.1, PW ID 1, state is down (local ready) PW class not set, XC ID 0x5000001 Encapsulation MPLS, protocol LDP PW type Ethernet, control word enabled, interworking none PW backup disable delay 0 sec

Sequencing not set MPLS Local Remote _____ Label 30005 unknown Group ID 0x5000300 Interface GigabitEthernet0/4/0/1 0×0 unknown MTU 1500 unknown Control word enabled unknown PW type Ethernet unknown VCCV CV type 0x2 0x0 (none) (LSP ping verification) VCCV CC type 0x3 0x0 (none) (control word) (router alert label) Create time: 20/11/2007 21:45:06 (00:53:31 ago) Last time status changed: 20/11/2007 22:38:14 (00:00:23 ago) Statistics: packet totals: received 0, sent 0 byte totals: received 0, sent 0 Backup PW: PW: neighbor 2.2.2.2, PW ID 2, state is up (established) Backup for neighbor 1.1.1.1 PW ID 1 (active) PW class not set, XC ID 0x0 Encapsulation MPLS, protocol LDP PW type Ethernet, control word enabled, interworking none PW backup disable delay 0 sec Sequencing not set MPLS Local Remote _____ ____ Label 30006 Group ID unassigned 16003 0x5000400 Interface unknown GigabitEthernet0/4/0/2 MTU 1500 1500 Control word enabled enabled PW type Ethernet Ethernet VCCV CV type 0x2 0x2 (LSP ping verification) (LSP ping verification) VCCV CC type 0x3 0x3 (control word) (control word) (router alert label) (router alert label) _____ Backup PW for neighbor 1.1.1.1 PW ID 1 Create time: 20/11/2007 21:45:44 (00:52:54 ago) Last time status changed: 20/11/2007 21:45:48 (00:52:49 ago) Statistics: packet totals: received 0, sent 0 byte totals: received 0, sent 0

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

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

Group VPWS, XC ac3, state is up; Interworking none AC: GigabitEthernet0/7/0/5.3, state is up Type VLAN; Num Ranges: 1 VLAN ranges: [12, 12] MTU 1508; XC ID 0x2440096; interworking none Statistics:

```
packets: received 26392092, sent 1336
bytes: received 1583525520, sent 297928
drops: illegal VLAN 0, illegal length 0
PW: neighbor 3.3.3.3, PW ID 3, state is up ( established )
PW class VPWS1, XC ID 0x2440096
Encapsulation MPLS, protocol LDP
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
Preferred path tunnel TE 3, fallback disabled
PW Status TLV in use
    MPLS
            Local
                                          Remote
     _____
     Label
               16147
                                          21355
               0x120001c0
     Group ID
                                          0x120001c0
                                         GigabitEthernet0/7/0/5.3
     Interface GigabitEthernet0/7/0/5.3
                1508
                                          1508
     MTU
     Control word disabled
                                          disabled
     PW type Ethernet
                                         Ethernet
                                         0x2
     VCCV CV type 0x2
               (LSP ping verification)
                                          (LSP ping verification)
     VCCV CC type 0x6
                                          0x6
                (router alert label)
                                          (router alert label)
                (TTL expiry)
                                          (TTL expiry)
     _____
                             _____
Incoming Status (PW Status TLV):
```

```
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 4294705365
Create time: 21/09/2011 08:05:01 (00:14:01 ago)
Last time status changed: 21/09/2011 08:07:01 (00:12:01 ago)
Statistics:
packets: received 1336, sent 26392092
bytes: received 297928, sent 1583525520
```

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

```
RP/0/RSP0/CPU0:router# show 12vpn xconnect interface pw-ether 67 detail
Group g1, XC xc1, state is down; Interworking none
 AC:PW-Ether1, state is up
   Type PW-Ether
   Interface-list: interfacelist1
   Replicate status:
     Gi0/2/0/1: success
     Gi0/3/0/1: pending
     Gi0/4/0/1: failed
   MTU 1500; interworking none
   Statistics:
     packets: received 0, sent 0
     bytes: received 0, sent 0
 PW: neighbor 130.130.130.130, PW ID 1234, state is down ( provisioned )
   PW class not set
   Encapsulation MPLS, protocol LDP
   PW type Ethernet VLAN, control word disabled, interworking none
   Sequencing not set
   Internal label: 16008
   VLAN id imposed: 101
     MPLS
                Local
                                             Remote
     -----
                                             _____
     Label 16001
                                             unknown
```

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

This table describes the significant fields shown in the display.

Table 6: show I2vpn xconnect Command Field Descriptions

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

This example shows the output of the **show l2vpn xconnect** command with IPv6 addresses listed:

RP/0/RSP0/CPU0:router# show 12vpn xconnect

```
Fri May 18 10:25:48.279 EDT
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
_____
                                  ___ _____
g1 xc1 DN Gi0/0/0/4.3 UP 1.2.3.4 1 DN
g1 xc2 UR Gi0/0/0/4.1 DN 1 UR
aaaa:bbbb::cdef
 -----
g1 xc3 UP Gi0/0/0/4.2 UP 1 UP
1111:2222::cdef
_____
g1 xc4 UR Gi0/0/0/4.4 DN 1 UR
1111:3333::4444
```

This example shows the output of the **show l2vpn xconnect interface** command:

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect interface Gi0/0/0/4.4 detail
```

```
Fri May 18 10:34:28.263 EDT
Group g1, XC xc4, state is unresolved; Interworking none
Not provisioned reason(s):
IPv6 not supported for this service
AC: GigabitEthernet0/0/0/4.4, state is down (Segment-down)
Type VLAN; Num Ranges: 1
VLAN ranges: [4, 4]
MTU 1500; XC ID 0x4; interworking none
PW: neighbor 1111:3333::4444, PW ID 1, state is unresolved
```

This example shows the output of the **show running-config l2vpn xconnect group** command with IPv6 neighbor information:

```
RP/0/RSP0/CPU0:router# show running-config l2vpn xconnect group g1 p2p xc4
```

```
Fri May 18 10:35:51.734 EDT
l2vpn
xconnect group g1
p2p xc4
interface GigabitEthernet0/0/0/4.4
neighbor ipv6 1111:3333::4444 pw-id 1
!
```

This example shows the output of the **show l2vpn xconnect neighbor ipv4** command:

RP/0/RSP0/CPU0:router# show 12vpn xconnect neighbor ipv4 1.2.3.4

This example shows the output of the **show l2vpn xconnect neighbor ipv6** command:

RP/0/RSP0/CPU0:router# show 12vpn xconnect neighbor ipv6 1111:2222::cdef

This example shows the output of the **show l2vpn xconnect neighbor ipv6** command:

RP/0/RSP0/CPU0:router# show l2vpn xconnect neighbor ipv6 1111:2222::cdef

Fri May 18 10:33:57.813 EDT Group g1, XC xc3, state is up; Interworking none AC: GigabitEthernet0/0/0/4.2, state is up Type VLAN; Num Ranges: 1 VLAN ranges: [2, 2] MTU 1500; XC ID 0x2; interworking none Statistics: packets: received 0, sent 0 bytes: received 0, sent 0 drops: MTU exceeded 0, other 0 PW: neighbor 1111:2222::cdef, PW ID 1, state is up PW class ts, XC ID 0x2 Encapsulation L2TPv3, protocol none Source address 1111:2222::abcd PW type Ethernet VLAN, control word disabled, interworking none PW backup disable delay 0 sec Sequencing not set L2TP class not set, IPv6 source address 1111:2222::abcd TOS 40 (reflect disabled), TTL 255, DF bit not set Path MTU: disabled L2TPv3 Local Remote _____ ____ Session 1 1 Cookie size 0 bytes 0 bytes Cookie unassigned unassigned ------Create time: 18/05/2012 07:40:08 (04:12:49 ago) Last time status changed: 18/05/2012 07:40:08 (04:12:49 ago) Statistics: packets: received 0, sent 0 bytes: received 0, sent 0

RP/0/RSP0/CPU0:router# show 12vpn xconnect neighbor ipv6 1111:2222::cdef detail

This example shows the output of the **show l2vpn xconnect state** commands:

RP/0/RSP0/CPU0:router# show 12vpn xconnect state up

```
Fri May 18 10:36:45.913 EDT
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
```

g1 xc3 UP Gi0/0/0/4.2 UP 1 UP 1111:2222::cdef

drops: out of sequence 0, other 0

RP/0/RSP0/CPU0:router# show 12vpn xconnect state down

RP/0/RSP0/CPU0:router# show 12vpn xconnect state unresolved

```
Fri May 18 10:37:30.610 EDT
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
g1 xc2 UR Gi0/0/0/4.1 DN 1 UR aaaa:bbbb::cdef
g1 xc4 UR Gi0/0/0/4.4 DN 1 UR 1111:3333::4444

Related Commands

L

Command

xconnect group, on page 167

no-statistics command.

Description 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 sav	ed to a specified file.
	list-CLIs	Specifies the list of CLIs but not execute	ed.
	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		and collects information for Layer 2 VPN p resentatives when troubleshooting a router	platform related issues that is useful for Cisco Technica r.
Note	The show t	ech-sunnort l2vnn platform command do	bes not collect all bridge domains information when

there is large scale values associated with bridge domains. Hence, use the show tech-support l2vpn platform

Task ID Task Operation ID

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 ipv6_address Source IPv6 address of pseudowire				
Syntax Description					
Command Default	None				
Command Modes	p2p pseudo	wire configuration			
Command History	Release	Modification			
	Release 4.3.1	This command was introduced			
Usage Guidelines		user group assignment is preve	er group associated with a task group that includes appropriate task enting you from using a command, contact your AAA administrator		
Note	All L2VPN	configurations can be deleted	l using the no l2vpn command.		

Task ID Task Operation ID

> 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 92	Enters p2p configuration submode to configure point-to-point cross-connects.
	neighbor (L2VPN), on page 76	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.

l

	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 dis	sabled by default.				
Command Modes	l2vpn bridge group	bridge-domain access circuit configuration				
Command History	Release Mod	ification				
	Release This 3.7.2	command was introduced.				
Usage Guidelines	Bridge Protoco	ol 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.					
		can only be programmed with a granularity of 8 pps, so values are not divisible by eight. aded to the nearest increment of eight.				
Task ID	Task Operations	-				
	l2vpn read, write	-				
Examples	The following example enables storm control thresholds throughout the bridge domain:					
	RP/0/RSP0/CPU0:a RP/0/RSP0/CPU0:a	9k1 # configure 9k1(config)# 12vpn 9k1(config-l2vpn) # bridge group BG1 9k1(config-l2vpn-bg) # bridge-domain BD1 9k1(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)# 12vpn
RP/0/RSP0/CPU0:a9k1(config-12vpn)# bridge group BG1
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd)# bridge-domain BD2
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd)# interface Bundle-Ether9001.2001
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-ac)# storm-control unknown-unicast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-ac)# storm-control multicast pps 100
RP/0/RSP0/CPU0:a9k1(config-12vpn-bg-bd-ac)# storm-control broadcast pps 100
```

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

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

Running Configuration

```
12vpn
bridge group BG1
 bridge-domain BD1
   storm-control unknown-unicast pps 100
   storm-control multicast pps 100
   storm-control broadcast pps 100
  1
  bridge-domain BD2
   interface Bundle-Ether9001.2001
    storm-control unknown-unicast pps 100
    storm-control multicast pps 100
   storm-control broadcast pps 100
   1
   neighbor 10.1.1.1 pw-id 20011001
    storm-control unknown-unicast pps 100
    storm-control multicast pps 100
    storm-control broadcast pps 100
   1
  !
 1
1
end
RP/0/RSP0/CPU0:a9k1(config)#
```

tag-impose

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

tag-impose vlan value

	no tag-impo	ose vlan value					
Syntax Description	vlan VLAN in tagged mode.						
	value Tag 0.	value. The range is from 1 t	to 4094. The default value is				
Command Default	None						
Command Modes	L2VPN conf	iguration					
Command History	Release	Modification					
	Release 4.2.	1 This command was introduced.					
Usage Guidelines		er group assignment is prev	•	group that includes appropriate task nd, contact your AAA administrator			
Task ID	Task Oper ID	ations					
	l2vpn read write						
Examples	This example shows how to specify a tag for a VLAN:						
	RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C		n) # xconnect group xcl	-			
Related Commands	Command		Description				
	pw-class (L2	2VPN), on page 84	Enters pseudowire class sul	bmode to define a pseudowire class			

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.

template.

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.							
	valueSets 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 packet is not an IPv4 or IPv6 packet, the COS fields are copied from the VLAN header, even if TOS is configured.							
Command Modes	L2VPN pseudowire class encapsulation L2TPv3 configuration							
Command History	Release Modification							
	ReleaseThis command was4.3.1introduced							
Usage Guidelines	To use this command, you must be in a user group associated with a task 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 Operation ID							
	l2vpn read, write							
	Example							
	This example shows how to configure TOS reflection:							
	<pre>RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# pw-class kanata01 RP/0/RSP0/CPU0:router(config-12vpn-pwc)# encapsulation 12tpv3 RP/0/RSP0/CPU0:router(config-12vpn-pwc-12tpv3)# protocol 12tpv3 RP/0/RSP0/CPU0:router(config-12vpn-pwc-12tpv3)# tos reflect</pre>							
	The following example shows how to set a TOS value:							
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# pw-class kanata01 RP/0/RSP0/CPU0:router(config-12vpn-pwc)# encapsulation 12tpv3							

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

Related Commands	Command	Description	
	pw-class (L2VPN), on page 84	Enters pseudowire class submode to define a pseudowire class template.	
	pw-class encapsulation l2tpv3, on page 85	Configures L2TPv3 pseudowire encapsulation.	

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	Config	gures Ethernet port mode	2.			
	vlan	vlan Configures VLAN tagged mode.					
	passthroug	gh Enable	es the pseudowires to pas	ss through the in	ncoming tags.		
Command Default	None						
Command Modes	L2VPN ps	eudowire	class MPLS encapsulati	on			
Command History	Release	Modi	ification				
	Release 3.	7.2 This	command was introduce	ed.			
	Release 4.	1.0 The v	variable passthrough wa	as introduced.			
Usage Guidelines		user grou	d, you must be in a user p assignment is preventi	0 1		· 1	11 1
Note	All L2VP	N configu	rations can be deleted us	ing the no l2vj	pn command.		
Task ID	Task O ID	perations					
	-	ead, rite					

Examples	This example shows how to configure Ethernet transport mode:					
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 1 RP/0/RSP0/CPU0:router(config-120 RP/0/RSP0/CPU0:router(config-120 RP/0/RSP0/CPU0:router(config-120	l 2vpn /pn)# pw-class kanata01				
	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)# J RP/0/RSP0/CPU0:router(config-12x RP/0/RSP0/CPU0:router(config-12x RP/0/RSP0/CPU0:router(config-12x	L 2vpn /pn)# pw-class pwc1				
Related Commands	Command	Description				
	pw-class (L2VPN), on page 84	Enters pseudowire class submode to define a pseudowire class				

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.

template.

		-	ode vlan passthrough mode vlan passthrough					
Syntax Descri	ption	This command	This command has no keywords or arguments.					
Command Def	ault	None	lone					
Command Mo	des	L2VPN bridge	2VPN bridge domain configuration					
Command Hist	tory	Release	Modification					
		Release 4.3.1	This command was introduced.					
Usage Guideli	nes	To use this command, you must be in a user group associated with a task 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 co	onfigurations can be deleted using	g 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)# 12vpn						
	RP/0/R	SP0/CPU0:rou	ter(config-l2v	<pre>rpn)# bridge group bg1 rpn-bg)# bridge-domain bd1 rpn-bg-bd)# transport mode vlan passthrough</pre>			
Related Commands	Comma	and		Description			
	bridge	-domain (VPLS	6), on page 176	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	<i>ttl_value</i> The TTL Value. Range is from 1 to 255.
Command Default	None
Command Modes	L2VPN pseudowire class encapsulation L2TPv3 configuration
Command History	Release Modification

ReleaseThis command was4.3.1introduced

Usage Guidelines To use this command, you must be in a user group associated with a task 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/F RP/0/F	RSP0/CPU0:r RSP0/CPU0:r	<pre>couter(config)# 12vpn couter(config-l2vpn)# pw-class kanata01 couter(config-l2vpn-pwc)# encapsulation 12tpv3 couter(config-l2vpn-pwc-l2tpv3)# protocol 12tpv3</pre>			
			router(config-l2vpn-pwc-l2tpv3)# ttl 40			
Related Commands	Comm	and	Description			
	pw-cl	ass (12\/PNI)	on page 84 Enters pseudowire class submode to d			

pw-class (L2VPN), on page 84	Enters pseudowire class submode to define a pseudowire class template.
pw-class encapsulation l2tpv3, on page 85	Configures L2TPv3 pseudowire encapsulation.

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.		

•					
N	ote You c	can configure u	p to a maximum of	16K cross-connects per bo)X.
Task ID	Task ID	Operations			
	l2vp	n read, write			
Examples	The f	ollowing exam	ple shows how to g	roup all cross -connects fo	r customer_atlantic:
	RP/0/	/RSP0/CPU0:ro	uter# configure uter(config)# 12 uter(config-12vp	vpn n)# xconnect group cus	tomer_atlantic
Related Command	ds Com	mand		Description	
	shov	v l2vpn xconne	ct, on page 145	Displays brief info	ormation on configured cross-connects.



Multipoint Layer 2 Services Commands

- action (VPLS), on page 170
- aging (VPLS), on page 172
- aps-channel, on page 173
- autodiscovery bgp, on page 175
- bridge-domain (VPLS), on page 176
- bridge group (VPLS), on page 177
- clear l2vpn bridge-domain (VPLS), on page 178
- debug l2vpn forwarding platform vpls all location, on page 179
- description (G.8032), on page 179
- dhcp ipv4 snoop profile (VPLS), on page 180
- ethernet ring g8032, on page 181
- ethernet ring g8032 profile, on page 182
- exclusion list, on page 184
- flooding disable, on page 185
- flooding unknown-unicast disable (VPLS), on page 186
- igmp snooping disable, on page 187
- inclusion-list, on page 188
- instance (G.8032), on page 189
- interface (VPLS), on page 190
- l2vpn resynchronize forwarding mac-address-table location, on page 191
- learning disable (VPLS), on page 192
- level, on page 193
- limit (VPLS), on page 194
- mac (VPLS), on page 196
- mac secure, on page 197
- maximum (VPLS), on page 198
- monitor interface (port0), on page 200
- monitor interface (port1), on page 201
- mpls static label (VPLS), on page 202
- mtu (VPLS), on page 203
- multicast p2mp, on page 204
- neighbor (VPLS), on page 206
- notification (VPLS), on page 207

- open ring, on page 208
- port0 interface, on page 209
- port1, on page 210
- port-down flush disable (VPLS), on page 211
- profile, on page 213
- pw-class, on page 214
- pw-oam, on page 215
- route-target, on page 216
- routed, on page 218
- rpl, on page 219
- show ethernet ring g8032, on page 220
- show l2vpn bridge-domain (VPLS), on page 223
- show l2vpn ethernet ring g8032, on page 245
- show l2vpn forwarding bridge-domain (VPLS), on page 247
- show l2vpn forwarding bridge-domain mac-address (VPLS), on page 253
- show l2vpn forwarding ethernet ring g8032, on page 258
- show l2vpn forwarding protection main-interface, on page 260
- show l2vpn protection main-interface, on page 261
- shutdown (Bridge Domain), on page 264
- shutdown (VFI), on page 265
- signaling-protocol, on page 266
- split-horizon group, on page 267
- static-address (VPLS), on page 268
- static-mac-address (VPLS), on page 269
- ten-propagation, on page 271
- time (VPLS), on page 271
- transport rsvp-te, on page 273
- type (VPLS), on page 274
- vfi (VPLS), on page 275
- withdraw (VPLS), on page 276

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 ad	dress 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 Operations ID					
	l2vpn read, write					
Examples	The following example shows how to when the number of MAC addresses	configure the bridge bar to flood all unknown unicast packets learned by the bridge reaches 10:				
	RP/0/RSP0/CPU0:router#configure RP/0/RSP0/CPU0:router(config)#1 RP/0/RSP0/CPU0:router(config-12 RP/0/RSP0/CPU0:router(config-12 RP/0/RSP0/CPU0:router(config-12 RP/0/RSP0/CPU0:router(config-12 RP/0/RSP0/CPU0:router(config-12	vpn)# bridge group 1 vpn-bg)# bridge-domain bar vpn-bg-bd)# mac vpn-bg-bd-mac)# limit vpn-bg-bd-mac-limit)# action flood				
Related Commands	Command	Description				
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.				
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.				

I

Command	Description
limit (VPLS), on page 194	Sets the MAC address limit for action, maximum, and notification and enters L2VPN bridge group bridge domain MAC limit configuration mode.
l2vpn, on page 69	Enters L2VPN configuration mode.
mac (VPLS), on page 196	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 198	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 207	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 271 and the type (VPLS), on page 274 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 Operations ID
	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 176	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then assigns network interfaces to the bridge domain.
	l2vpn, on page 69	Enters L2VPN configuration mode.
	mac (VPLS), on page 196	Enters L2VPN bridge group bridge domain MAC configuration mode.
	time (VPLS), on page 271	Configures the maximum aging time.
	type (VPLS), on page 274	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 | GigabitEthernet | 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.

I

	interfac	e	-	iated to port0 or port1. You can assign one of these interfaces:
			• Bundle Ethernet	
			• Fast Ethernet	
			Gigabit Ethernet	
			TenGigabit Ethern	net
	bridge-	domain	Specifies VPLS domain	n where virtual channel is connected.
	none		Specify APS channel p	ort0 or port1 as none.
	xconneo	et	Specifies VPWS xconn	nect where virtual channel is connected.
Command Default	None			
Command Modes	L2VPN	configur	ation mode	
Command History	Release	M	odification	
	Release 4.1.0		is command was troduced.	
Usage Guidelines Task ID	IDs. If th for assist	e user g	roup assignment is preve	ser group associated with a task group that includes appropriate task enting you from using a command, contact your AAA administrator
	ID	operation	•	
	l2vpn i	read, write	_	
	This exa	mple sho	- ows how to configure G.	8032 instance APS channel:
	RP/0/RSI RP/0/RSI RP/0/RSI RP/0/RSI RP/0/RSI RP/0/RSI RP/0/RSI	P0/CPU0 P0/CPU0 P0/CPU0 P0/CPU0 P0/CPU0 P0/CPU0 P0/CPU0 P0/CPU0	:router(config-l2vpn :router(config-l2vpn :router(config-l2vpn :router(config-l2vpn :router(config-l2vpn)# ethernet ring g8032 r1 -erp)# instance 1 -erp-instance)# description test -erp-instance)# profile p1 -erp-instance)# rpl port0 neighbor -erp-instance)# inclusion-list vlan-ids e-g -erp-instance)# aps-channel
Related Commands	Commai	nd		Description
	etherne	t ring g8l	032, on page 181	Enables G.8032 ring mode and enters the G.8032 configuration

submode.

Command	Description
inclusion-list, on page 188	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.

	autodiscove no autodise		
Syntax Description	This comma	nd has no keywords or arg	uments.
Command Default	None.		
Command Modes	VFI configu	ration	
Command History	Release	Modification	
	Release 3.7	2 This command was introduced.	
Usage Guidelines		ser group assignment is pre	user group associated with a task group that includes appropriate task eventing you from using a command, contact your AAA administrator
Task ID	Task Ope ID	rations	
	l2vpn read writ		
Examples	The followin	ng example shows how to c	configure a bridge domain:
	RP/0/RSP0/0 RP/0/RSP0/0 RP/0/RSP0/0 RP/0/RSP0/0	CPU0:router(config-l2vg CPU0:router(config-l2vg	on)# bridge group EGroup on-bg)# bridge-domain eastdomain
Related Commands	Command		Description
	bridge-dom	ain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge grou	p (VPLS), on page 177	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 69	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-dom no bridge-domain bridge-	
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 configu	ration
Command History	Release Modification	
	Release 3.7.2 This comman	d was introduced.
Usage Guidelines Task ID	Use the bridge-domain com Task Operations ID 12vpn read,	mand to enter L2VPN bridge group bridge domain configuration mode.
	write	
Examples	The following example show	s how to configure a bridge domain:
		nfig)# 12vpn nfig-12vpn)# bridge group 1 nfig-12vpn-bg)# bridge-domain bar
Related Commands	Command	Description
	bridge group (VPLS), on page	e 177 Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	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 bridg	ge group to which the interface belongs.
Command Default	No bridge gro	oup is created.	
Command Modes	L2VPN confi	guration	
Command History	Release	Modification	
	Release 3.7.2	2 This command was introduced.	
Usage Guidelines		er group assignment is prev	user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator
	Use the bridg	ge group command to ente	r L2VPN bridge group configuration mode.
Task ID	Task Opera ID	tions	
	l2vpn read, write		
Examples	The following	g example shows that bridg	ge group 1 is assigned:
	RP/0/RSP0/C RP/0/RSP0/C	PU0:router# configure PU0:router(config)# 12 PU0:router(config-l2vp; PU0:router(config-l2vp;	n)# bridge group 1
Related Commands	Command		Description
	bridge-doma	in (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	l2vpn, on pag	je 69	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 brid	dge domains on the router.
	bd-name name	Clears and restarts the specif the bridge-domain.	ied bridge domain. The name argument specifies the name of
	group group	Clears and restarts all the brid	dge 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			
Usage Guidelines	IDs. If the user for assistance. This is the met	group assignment is preventin	
Usage Guidelines Task ID	IDs. If the user for assistance. This is the met	group assignment is preventing thod that allows a bridge to for configured MAC limit.	g you from using a command, contact your AAA administrator
	IDs. If the user for assistance. This is the met exceeding the Task Operation	group assignment is preventing thod that allows a bridge to for configured MAC limit.	g you from using a command, contact your AAA administrator
	IDs. If the user for assistance. This is the met exceeding the Task Operati ID 12vpn read, write	group assignment is preventing thod that allows a bridge to for configured MAC limit.	g you from using a command, contact your AAA administrator
Task ID	IDs. If the user for assistance. This is the met exceeding the or Task Operati ID 12vpn read, write The following on the router:	group assignment is preventing thod that allows a bridge to for configured MAC limit.	the MAC addresses and to restart all the bridge domains
Task ID	IDs. If the user for assistance. This is the met exceeding the or Task Operati ID 12vpn read, write The following on the router:	example shows how to clear all	g you from using a command, contact your AAA administrator ward again after it was put in Shutdown state as a result of the MAC addresses and to restart all the bridge domains

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 inf	ormation.			
Command Default	None						
Command Modes	EXEC						
Command History	Release	Modificati	on				
	Release 5.1	This comm introduced					
Usage Guidelines		user group as	ou must be in a user ssignment is prevent				
Task ID	Task ID	Operation					
	root-systen	n 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	Releas	e Mo	dification	
	Releas 4.1.0		s command was oduced.	
Usage Guidelines		the user gro		user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator
Task ID	Task ID	Operation		
	12vpn	read,		
		write		
			ws how to specify a de	escription for G.8032 Ethernet ring instance:
	This ex RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R	ample show SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0:	router# configure router(config)# 12 router(config-12vpr router(config-12vpr router(config-12vpr	<pre>vpn n)# ethernet ring g8032 r1 n-erp)# instance 1 n-erp-instance)# description test</pre>
	This ex RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R	ample show SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0:	router# configure router(config)# 12 router(config-12vpr router(config-12vpr	<pre>vpn n) # ethernet ring g8032 r1 n-erp)# instance 1 n-erp-instance)# description test n-erp-instance)#</pre>
Related Commands	This ex RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R	ample show SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0:	router# configure router(config)# 12 router(config-12vpr router(config-12vpr router(config-12vpr	<pre>vpn n)# ethernet ring g8032 r1 n-erp)# instance 1 n-erp-instance)# description test</pre>
Related Commands	This ex RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R Comm	ample show SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0:	router# configure router(config)# 12 router(config-12vpr router(config-12vpr router(config-12vpr	<pre>vpn n) # ethernet ring g8032 r1 n-erp)# instance 1 n-erp-instance)# description test n-erp-instance)#</pre>
Related Commands	This ex RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R RP/0/R Comm 12vpn,	ample show SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0: SP0/CPU0: and on page 69	router# configure router(config)# 12 router(config-12vpr router(config-12vpr router(config-12vpr	<pre>vpn n)# ethernet ring g8032 r1 n-erp)# instance 1 n-erp-instance)# description test n-erp-instance)# Description</pre>

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 grou	p 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 tasl IDs. If the user group assignment is preventing you from using a command, contact your AAA administrato for assistance.						
Task ID	Task Op ID	erations					
	l2vpn rea wr						
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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group 1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# dhcp ipv4 snoop profile attach This example shows how to enable DHCP snooping over a pseudowire:						
	RP/0/RSP0 RP/0/RSP0 RP/0/RSP0 RP/0/RSP0 RP/0/RSP0 RP/0/RSP0	/CPU0:router(config-12v /CPU0:router(config-12v /CPU0:router(config-12v	L2vpn /pn)# bridge group 1 /pn-bg)# bridge-domain bar /pn-bg-bd)# vfi vf1				
Related Commands	Command		Description				
	bridge-doi	main (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.				
	bridge gro	up (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.				
	I2vpn, on page 69 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

Syntax Description	protocol ring identifier Ring profile name. The maximum size of the profile name is 32 characters.					
Command Default	None					
Command Modes	L2VPN con	ifiguration mode				
Command History	Release	Modification				
	Release 4.1.0	This command was introduced.				
Usage Guidelines		ser group assignment is	in a user group associated with a task group that includes appropriate task preventing you from using a command, contact your AAA administrator			
Task ID	Task Ope ID	eration				
	l2vpn read, write					
	Example					
	This example shows how to enable the G.8032 ring mode:					
	RP/0/RSP0/ RP/0/RSP0/	'CPU0:router# configur 'CPU0:router(config)# 'CPU0:router(config-1 'CPU0:router(config-1	<pre>#12vpn L2vpn)#ethernet ring g8032 p1</pre>			
Related Commands	Command		Description			
	exclusion li	ist, on page 184	Defines a set of Virtual LAN (VLAN) IDs that are not protected by the Ethernet ring protection mechanism.			
	instance (G	3.8032), on page 189	Configures a G.8032 Ethernet ring instance and enters Ethernet ring G.8032 instance configuration submode.			
	port0 interf	ace, on page 209	Enables G.8032 for a specified ring port.			
	port1, on pa	age 210	Enables G.8032 for a specified ring port.			

no ethernet ring g8032 protocol ring identifier

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.

I

Syntax Description	non-rever	tive	Configure	Configures non-revertive ring instance.			
	timer		Configure	Configures G.8032 timer. 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.			
	guard		the defaul				
	hold-off		and the de	 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. 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. 			
	wtr		operator, a				
Command Default	None						
Command Modes	-						
Command History	Release	Modification		-			
	Release 4.1.0	This command w introduced.	vas	_			
Usage Guidelines				group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator			
Task ID	Task ID	Operation					
	ethernet-ser	vices read, write					
	This example shows you how to configure a G.8032 ring profile:						
	RP/0/RSP0/CPU0:router# config RP/0/RSP0/CPU0:router(config) RP/0/RSP0/CPU0:router(config-		fig)# ethern	g)# ethernet ring g8032 profile p1			
	RP/0/RSP0,	0100.100001 (0001					
Related Commands	Command			Description			

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

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 HistoryReleaseModificationReleaseThis command was4.1.0introduced.

Usage Guidelines

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

 Task ID
 Task Dperation

 ID
 12vpn read, write

This example shows the output from the exclusion list command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-12vpn-erp)# exclusion-list vlan-ids e-g
RP/0/RSP0/CPU0:router(config-12vpn-erp)#
```

Related Commands	Command	Description
	ethernet ring g8032, on page 181	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 dis no flooding					
	This comman	nd has no keywords or arg	guments.			
Command Default	The default b	behavior is that packets ar	e flooded when their destination MAC address is not found.			
Command Modes	L2VPN bridg	ge group bridge domain c	onfiguration			
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 floodin discarded.	ng is disabled, all unknow	n unicast packets, all broadcast packets, and all multicast packets are			
Task ID	Task Oper ID	ations				
	l2vpn read write					
Examples	The following example shows how to disable flooding on the bridge domain called bar:					
	RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C	-	2vpn			
Related Commands	Command		Description			
	bridge-doma	ain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.			

Command	Description
bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 69	Enters L2VPN configuration mode.
mtu (VPLS), on page 203	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 This command has no keywords or arguments. Syntax Description The default behavior is that packets are flooded when their destination MAC address is not found. **Command Default** L2VPN bridge group bridge domain configuration **Command Modes Command History** Release Modification Release 3.9.0 This command was introduced. To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** 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 Operations ID 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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group 1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# flooding unknown-unicast disable				
Related Commands	Command	Description			
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.			
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.			
	l2vpn, on page 69	Enters L2VPN configuration mode.			
	mtu (VPLS), on page 203	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	p bridge domain configuration	
Command History	Releas	e Modifi	cation	
	Release	e 5.1 This co	ommand was introduced.	
Usage Guidelines		he user group	d, you must be in a user group associated with a task group that includes appropriate task p assignment is preventing you from using a command, contact your AAA administrator	
Task ID	Task ID	Operations		
	l2vpn	read, write		
Examples	This exa	ample shows	s 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 69	Enters L2VPN configuration mode.		
	bridge group (VPLS), on page 177	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 176	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-idsvlan-id no inclusion-list vlan-idsvlan-id

Syntax Description	vlan-ids	Associates a set of VLAN IDs	with the current instance.
	vlan-id	List of VLAN IDs in the form	/lan-id <vlan range="">[,<vlan range="" range][,<vlan="">][,<vlan range="">][,</vlan></vlan></vlan>
Command Default	None		
Command Modes	Ethernet rin	ng G.8032 instance configurati	on submode
Command History	Release	Modification	
	Release 4.1.0	This command was introduced.	
Usage Guidelines		user group assignment is preve	er group associated with a task group that includes appropriate task nting you from using a command, contact your AAA administrator
Task ID	Task Op ID	eration	
	l2vpn rea wr		

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

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# ethernet ring g8032 r1
RP/0/RSP0/CPU0:router(config-12vpn-erp)# instance 1
RP/0/RSP0/CPU0:router(config-12vpn-erp-instance)# description test
RP/0/RSP0/CPU0:router(config-12vpn-erp-instance)# profile p1
RP/0/RSP0/CPU0:router(config-12vpn-erp-instance)# rpl port0 neighbor
RP/0/RSP0/CPU0:router(config-12vpn-erp-instance)# inclusion-list vlan-ids e-g
```

	·		
Related Commands	Command	Description Enters L2VPN configuration mode.	
	l2vpn, on page 69		
	ethernet ring g8032, on page 181	Enables G.8032 ring mode and enters the G.8032 configuration submode.	
	instance (G.8032), on page 189	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 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.

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

Task ID Task Operation ID

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 181	Enables G.8032 ring mode and enters the G.8032 configuration submode.
	l2vpn, on page 69	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	<i>type</i> Interface type. For more information, use the question mark (?) online help function.			
	interface-path-ic	d 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 function	e information about the syntax for the router, use the question mark (?) online help	
Command Default	None			
Command Modes	L2VPN bridge	group brid	ge domain configuration	
Command History	Release	Modificati	on	
	Release 3.7.2	This comm introduced		

Usage GuidelinesTo use this command, you must be in a user group associated with a task 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:						
	<pre>RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn 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)#</pre>						
Related Commands	Comm	and		Description			
	bridge-domain (VPLS), on page 176		S), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.			
	bridge	group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.			
	l2vpn,	on page 69		Enters L2VPN configuration mode.			

I2vpn 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.

12vpn 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		er group assignment is preven	r group associated with a task group that includes appropriate task ting you from using a command, contact your AAA administrator				
	To ensure that correct information is displayed, enter this command before issuing any show commands for the mac address tables.						
Task ID	learn informa especially wh command bac addresses is u time is one m four minutes	tion from the network process een there are 512K MACs. The ek to back. The throttle time d under 16K MACs, the throttle	c-address-table location command initiates the transfer of MAC sors, to the L2FIB manager. This operation is CPU intensive erefore, the command is throttled, so that you cannot issue this epends on the number of MAC addresses. If the number of MAC time is five seconds. If it is between 16K and 128K, the throttle K and 256K, the throttle time is two minutes. The throttle time is 5K.				
	ID						
	l2vpn read, exect						
Examples	The following example shows how to retrieve the MAC address table from the network processors:						
	RP/0/RSP0/C	PU0:router# 12vpn resynch	ronize forwarding mac-address-table location 0/4/CPU0				
Related Commands	Command		Description				
	show l2vpn f	orwarding, on page 117	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.

Image: Syntax DescriptionImage: Image: I

Command Modes	L2VPN bridg	e group bridge domain M	IAC configuration			
Command History	Release	Modification				
	Release 3.7.2	This command was introduced.				
Usage Guidelines		r group assignment is pro	user group associated with a task group that includes appropriate task eventing you from using a command, contact your AAA administrator			
	When set, the learning disable command stops all MAC learning either on the specified interface or the bridge domain.					
Task ID	Task Opera ID	tions				
	l2vpn read, write					
Examples			ng is disabled on all ports in the bridge domain called bar, bridge unless the interface has its own MAC learning enable			
	RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI	PU0:router(config-l2v	pn)# bridge group 1 pn-bg)# bridge-domain bar			
Related Commands	Command		Description			
	bridge-domain (VPLS), on page 176		Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.			
		(\/PLS) on page 177	Creates a bridge group so that it can contain bridge domains and			
	bridge group	(VFL3), on page 177	then to assign network interfaces to the bridge domain.			
	bridge group I2vpn, on pag					

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	<i>number</i> The APS message level. The range is from between 0 to 7.					
Command Default	None					
Command Modes	Ethernet rir	ng G.8032 instance aps-channe	l configuration submode			
Command History	Release	Modification				
	Release 4.1.0	This command was introduced.				
Usage Guidelines		iser group assignment is preven	er group associated with a task group that includes appropriate task nting you from using a command, contact your AAA administrator			
Task ID	Task Ope ID	eration				
	l2vpn rea wr					
	This example shows how to enable the G.8032 ring mode:					
	RP/0/RSP0, RP/0/RSP0, RP/0/RSP0, RP/0/RSP0, RP/0/RSP0, RP/0/RSP0, RP/0/RSP0,	/CPU0:router(config-l2vpn- /CPU0:router(config-l2vpn- /CPU0:router(config-l2vpn- /CPU0:router(config-l2vpn-	<pre># ethernet ring g8032 r1 erp)# instance 1 erp-instance)# description test</pre>			
Related Commands	Command		Description			
	l2vpn, on p	age 69	Enters L2VPN configuration mode.			

limit	(VPLS)	

ethernet ring g8032, on page 181

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.

submode.

Enables G.8032 ring mode and enters the G.8032 configuration

	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				
		PN bridge group bridge domain MAC limit configuration mode. The log message is sent or a corresponding trap is generated with the MAC				
Task ID	Task Operations ID					
	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(config-12)	L2vpn /pn)# bridge group 1 /pn-bg)# bridge-domain bar /pn-bg-bd)# mac				
Related Commands	Command	Description				
	action (VPLS), on page 170	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.				
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.				

Command	Description
l2vpn, on page 69	Enters L2VPN configuration mode.
mac (VPLS), on page 196	Enters L2VPN bridge group bridge domain MAC configuration mode.
maximum (VPLS), on page 198	Configures the specified action when the number of MAC addresses learned on a bridge is reached.
notification (VPLS), on page 207	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 Operat ID	ions				
	l2vpn read, write					
Examples	The following mode:	example shows how to enter L?	L2VPN bridge group bridge domain MAC configuration			
	RP/0/RSP0/CP	U0:router# configure U0:router(config)# 12vpn U0:router(config-12vpn)# 1	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)#

Command	Description
aging (VPLS), on page 172	Enters the MAC aging configuration submode to set the aging parameters such as time and type.
bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 69	Enters L2VPN configuration mode.
learning disable (VPLS), on page 192	Overrides the MAC learning configuration of a parent bridge or sets the MAC learning configuration of a bridge.
limit (VPLS), on page 194	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 268	Adds static entries to the MAC address for filtering.
withdraw (VPLS), on page 276	Disables MAC address withdrawal for a specified bridge domain
	aging (VPLS), on page 172 bridge-domain (VPLS), on page 176 bridge group (VPLS), on page 177 l2vpn, on page 69 learning disable (VPLS), on page 192 limit (VPLS), on page 194 static-address (VPLS), on page 268

mac secure

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

mac secure {ac	ction [{ none shutdown restrict}] logging disable}	
no mac secure	{action [{ none shutdown}] logging disable}	

Syntax Description	action	(Optional) Indicates the action to be taken when security is violated.		
	none Forwards the violating packet and allows the MAC address to b			
	shutdown Shuts down the violating bridge port.			
	restrict Drops the violating packet and disables the learn attempt.			
		Note The restrict keyword in applicable to interfaces only.		
	logging	(Optional) Enables logging.		
	disable	(Optional) Disables mac security.		
Command Default		address has been learned on a secure port and a relearn attempt from anoth		

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

Command Modes	l2vpn bridge group bridge domain configuration				
Command History	Relea	se Mod	ification		
	Releas 4.0.1	-	command was duced.		
Usage Guidelines	This co	ommand has	no keywords or arguments.		
Task ID	Task ID	Operations			
	l2vpn	Read, write			
Examples	This ex	ample show	vs how to enable mac security on bridge bar.		
	<pre>RP/0/RSP0/CPU0:router#configure RP/0/RSP0/CPU0:router(config)#12vpn RP/0/RSP0/CPU0:router(config-12vpn)#bridge group b1 RP/0/RSP0/CPU0:router(config-12vpn-bg)#bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)#mac secure RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-mac-secure)# This example shows how to shut down a violating bridge port on bridge bar:</pre>				
	<pre>RP/0/RSP0/CPU0:router#configure RP/0/RSP0/CPU0:router(config)#12vpn RP/0/RSP0/CPU0:router(config-12vpn)#bridge group b1 RP/0/RSP0/CPU0:router(config-12vpn-bg)#bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)#mac secure RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-mac-secure)#action shutdown RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-mac-secure)#</pre>				
Related Commands	Command		Description		
	bridge	-domain (VF	PLS), on page 176 Establishes a bridge domain, and enters L2VPN bridge group bridg domain configuration mode.		
	bridge group (VPLS), on page 177		S), on page 177 Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.		
	l2vpn,	on page 69	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	<i>value</i> Maximum number of learned MAC addresses.		
	For Release 5.1.0, the range is	from 5 to 512000.	
	For Release 5.1.1, the range is	from 5 to 128000.	
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 int	roduced.	
Usage Guidelines	sage Guidelines To use this command, you must be in a user group associated with a task group that includes approvide the user group assignment is preventing you from using a command, contact your AAA addressing for assistance.		
	The action can either be flood, no floot trap notification, or both are issued.	od, or shutdown. Depending on the configuration, a syslog, an SNMP	
Task ID	Task Operations ID		
	l2vpn read, write		
Examples	The following example shows when the and the bridge stops learning but cont	he number of MAC address learned on the bridge reaches 5000 tinues flooding:	
	RP/0/RSP0/CPU0:router# configur RP/0/RSP0/CPU0:router(config)#	12vpn	
		vpn-bg)# bridge-domain bar vpn-bg-bd)# mac	
Related Commands	Command	Description	
	action (VPLS), on page 170	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.	
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.	
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.	
	l2vpn, on page 69	Enters L2VPN configuration mode.	

Command	Description
limit (VPLS), on page 194	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 196	Enters L2VPN bridge group bridge domain MAC configuration mode.
notification (VPLS), on page 207	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 HistoryReleaseModificationReleaseThis command was4.1.0introduced.

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

 Task ID
 Task Operation

 ID
 12vpn 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

I

Command	Description	
l2vpn, on page 69	Enters L2VPN configuration mode.	
ethernet ring g8032, on page 181	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*

interface-name	Name of the monitored interface. The monitored interface must be a sub-interface of the main interface.
Configured phys	sical Ethernet or ether bundle interface
Ethernet ring g80	032 port1 submode
Release M	lodification
	his command was htroduced.
	nand, you must be in a user group associated with a task group that includes appropriate task group assignment is preventing you from using a command, contact your AAA administrator
Task Operation ID	n
l2vpn read, write	_
	Configured phys Ethernet ring g8 Release M Release T 4.1.0 in To use this comm IDs. If the user g for assistance. Task Operatio ID I2vpn read,

This example shows the output from the monitor interface command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# ethernet ring g8032 g1
RP/0/RSP0/CPU0:router(config-12vpn-erp)# port1 interface TenGigE 0/4/0/0
RP/0/RSP0/CPU0:router(config-12vpn-erp-port1)# monitor interface GigabitEthernet 0/0/1/0
```

RP/0/RSP0/CPU0:router(config-l2vpn-erp-port1)#

Related Commands

s	Command	Description	
	l2vpn, on page 69	Enters L2VPN configuration mode.	
	ethernet ring g8032, on page 181	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	Config	gures the remote pseudowire label.
	value	Note	The range of values for the remote labels depends on the label allocator of the remote router.
Command Default	By default, the	he router	attempts to assign dynamic labels to the pseudowire.
Command Modes	L2VPN brid	ge group	bridge domain Access/VFI pseudowire configuration
Command History	Release	Modi	fication
	Release 3.7.	2 This c introd	command was luced.
Usage Guidelines	IDs. If the us for assistance	er group e.	, you must be in a user group associated with a task group that includes appropriate task assignment is preventing you from using a command, contact your AAA administrator s of the pseudowire have matching static labels.
Task ID	Task Oper ID	ations	
	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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group 1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# vfi model RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000 RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000 RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000

Related Commands	Command	Description
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	Enters L2VPN configuration mode.
	neighbor (VPLS), on page 206	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
	pw-class , on page 214	Configures the pseudowire class template name to use for the pseudowire.
	vfi (VPLS), on page 275	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 mtuSyntax Descriptionbytes MTU size, in bytes. The range is from 46 to 65535.Command DefaultThe default MTU value is 1500.Command ModesL2VPN bridge group bridge domain configurationCommand HistoryReleaseRelease 3.7.2This command was introduced.

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

Task

ID

Operations

Bridge wide MTU is not enforced on the data traffic.

Task ID

Examples

Related Commands	Command	Description
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	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 185	Configures flooding for traffic at the bridge domain level or at the bridge port level.
	l2vpn, on page 69	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 sel	ection		
	transport	Specifies the transport type select	ion		
Command Default	None				
Command Modes	L2VPN bridge group	bridge domain VFI configuration			
Command History	Release Modifica	ation			
	ReleaseThis corr5.1introduct	nmand was ed.			
Usage Guidelines			ated with a task group that includes appropriate task using a command, contact your AAA administrator		
Task ID	Task Operation ID				
	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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group 1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# vfi v1 RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi)# multicast p2mp RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi-p2mp)#				
Related Commands	Command		Description		
	transport rsvp-te, or	n page 273	Enables RSVP-TE as transport on a VFI.		
	vfi (VPLS), on page	275	Configures virtual forwarding interface (VFI) parameters.		

bridge-domain (VPLS), on page 176

bridge group (VPLS), on page 177

l2vpn, on page 69

Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.

Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to

Enters L2VPN configuration mode.

the bridge domain.

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 brid	ge group bridge domain configuration
	L2VPN bric	lge group bridge domain VFI configuration
Command History	Release	Modification
	Release 3.7	.2 This command was introduced.
Usage Guidelines		command, you must be in a user group associated with a task group that includes appropriate task ser group assignment is preventing you from using a command, contact your AAA administrator ce.
		ghbor command to enter L2VPN bridge group bridge domain VFI pseudowire configuration natively, use the neighbor command to enter L2VPN bridge group bridge domain access pseudowire n mode.
Task ID	Task Ope ID	rations
	l2vpn read wri	
Examples		ng example shows how to configure an access pseudowire directly under a bridge domain ridge group bridge domain configuration mode:
	RP/0/RSP0/ RP/0/RSP0/ RP/0/RSP0/ RP/0/RSP0/	CPU0:router# configure CPU0:router(config)# 12vpn CPU0:router(config-12vpn)# bridge group 1 CPU0:router(config-12vpn-bg)# bridge-domain bar CPU0:router(config-12vpn-bg-bd)# neighbor 10.1.1.2 pw-id 1000 CPU0:router(config-12vpn-bg-bd-pw)#

L

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)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# bridge group 1
RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar
RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# vfi v1
RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi-pw)#
```

Related Commands	Command	Description		
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.		
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.		
	l2vpn, on page 69	Enters L2VPN configuration mode.		
	mpls static label (VPLS), on page 202	Configures the MPLS static labels and the static labels for the access pseudowire configuration.		
	pw-class , on page 214	Configures the pseudowire class template name to use for the pseudowire.		
	static-mac-address (VPLS), on page 269	Configures the static MAC address to associate a remote MAC address with a pseudowire or any other bridge interface.		
	vfi (VPLS), on page 275	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

VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers, IOS XR Release 6.4.x

0						
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 me notification		is generated. Alternatively, an SNMP trap is generated. Finally, no			
Task ID	Task Oper ID	ations				
	l2vpn read writ					
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/RSP0/0 RP/0/RSP0/0 RP/0/RSP0/0 RP/0/RSP0/0 RP/0/RSP0/0	CPU0:router(config-12 CPU0:router(config-12	12vpn vpn)# bridge group 1 vpn-bg)# bridge-domain bar vpn-bg-bd)# mac			
Related Commands	Command		Description			
	action (VPL	S), on page 170	Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.			
	bridge-dom	ain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.			
	bridge grou	p (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.			
	l2vpn, on pa	ge 69	Enters L2VPN configuration mode.			
	mac (VPLS)	, on page 196	Enters L2VPN bridge group bridge domain MAC configuration mode.			
	maximum (V	/PLS), on page 198	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-rii	ng			
	This command has no keywords or arguments.				
Command Default	The default	value is FALSE.			
Command Modes	Ethernet rin	g g8032 configuration submo	ode		
Command History	Release	Modification			
	Release 4.1.0	This command was introduced.			
Usage Guidelines		iser group assignment is preve	ser group associated with a task group that includes appropriate task enting you from using a command, contact your AAA administrator		
Task ID	Task Ope ID	eration			
	l2vpn rea wri				
	Example This example shows the output from the open-ring command:				
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# ethernet ring g8032 g1 RP/0/RSP0/CPU0:router(config-12vpn-erp)# open-ring RP/0/RSP0/CPU0:router(config-12vpn-erp)#				
Related Commands	Command		Description		
	l2vpn, on p	age 69	Enters L2VPN configuration mode.		
	ethernet ri	ng g8032, on page 181	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

I

Syntax Description	<i>interface name</i> 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 g80	032 configuration port0 submode			
Command History	Release M	lodification			
		his command was troduced.			
Usage Guidelines		nand, you must be in a user group associated with a task group that includes appropriate task group assignment is preventing you from using a command, contact your AAA administrator			
Task ID	Task Operation	n			
	l2vpn read, write	_			
	Example				
	This example shows the output from the port0 interface command:				
	RP/0/RSP0/CPU0 RP/0/RSP0/CPU0 RP/0/RSP0/CPU0	<pre>:router# configure :router(config)# l2vpn :router(config-l2vpn)# ethernet ring g8032 g1 :router(config-l2vpn-erp)# port0 interface Bundle-Ether 555 :router(config-l2vpn-erp-port0)#</pre>			
Related Commands	Command	Description			

d Commands	Command	Description
	l2vpn, on page 69	Enters L2VPN configuration mode.
	ethernet ring g8032, on page 181	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 rin	g g8032 configuration port1	submode		
Command History	Release	Modification			
	ReleaseThis command was4.1.0introduced.				
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropria IDs. If the user group assignment is preventing you from using a command, contact your AAA admini for assistance.				
Task ID	Task Ope ID	ration			
	l2vpn read writ				
	This example shows the output from the port1 command:				
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# RP/0/RSP0/CPU0:router(config-12vpn-er RP/0/RSP0/CPU0:router(config-12vpn-er		n)# ethernet ring g8032 g1 n-erp)# port1 interface TenGigE 0/6/0/3		
Related Commands	Command		Description		
	l2vpn, on pa	age 69	Enters L2VPN configuration mode.		
			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 po	rt-down flush disable				
Syntax Description	This command has no keywords or arguments.					
Command Default	None					
Command Modes	L2VPN	l bridge group bridge dom	nain MAC configuration			
Command History	Releas	se Modification				
	Releas	se 3.9.0 This command wa introduced.	as			
Usage Guidelines		the user group assignment	be in a user group associated with a task group that includes appropriate task t is preventing you from using a command, contact your AAA administrator			
	The po	ort-down flush disable co	mmand 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/R RP/0/R RP/0/R RP/0/R	SP0/CPU0:router(config SP0/CPU0:router(config	g)# 12vpn g-12vpn)# bridge group 1 g-12vpn-bg)# bridge-domain bar			
Related Commands	Comm	and	Description			
	action (VPLS), on page 170		Configures bridge behavior when the number of learned MAC addresses reaches the MAC limit configured.			
	bridge	-domain (VPLS), on page 1	176 Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.			
	bridge	group (VPLS), on page 17	7 Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.			
	l2vpn,	on page 69	Enters L2VPN configuration mode.			
	mac (\	/PLS), on page 196	Enters L2VPN bridge group bridge domain MAC configuration mode.			
	maxim	um (VPLS), on page 198	Configures the specified action when the number of MAC addresses learned on a bridge is reached.			

Command	Description
notification (VPLS), on page 207	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-	ıame			
Syntax Description	profile-name	<i>profile-name</i> Ethernet ring G.8032 profile name.			
Command Default	None				
Command Modes	Ethernet ring G.	8032 instance configuration submode			
Command History	Release N	Iodification			
		his command was atroduced.			
Usage Guidelines		nand, you must be in a user group associated with a task group that includes appropriate task group assignment is preventing you from using a command, contact your AAA administrator			
Task ID	 Task Operatio ID	n			
	l2vpn read, write	_			
	Example				
	This example shows how to specify a G.8032 ring profile name:				
	RP/0/RSP0/CPU0 RP/0/RSP0/CPU0 RP/0/RSP0/CPU0 RP/0/RSP0/CPU0 RP/0/RSP0/CPU0	<pre>D:router#configure D:router(config)# 12vpn D:router(config-12vpn)# ethernet ring g8032 r1 D:router(config-12vpn-erp)# instance 1 D:router(config-12vpn-erp-instance)# description test D:router(config-12vpn-erp-instance)# profile p1 D:router(config-12vpn-erp-instance)#</pre>			
Related Commands	Command	Description			

ted Commands	Command	Description	
	l2vpn, on page 69	Enters L2VPN configuration mode.	

Command	Description
ethernet ring g8032, on page 181	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-n	<i>ame</i> Pse nan	udowire class ne.	
Command Default	None			
Command Modes	L2VPN	N bridge	group bridge domain	n Access pseudowire configuration
Command History	Releas	se	Modification	
	Releas		This command was introduced.	
Usage Guidelines	IDs. If			in a user group associated with a task group that includes appropriate task preventing you from using a command, contact your AAA administrator
Task ID	Task ID	Operatio	ns	
	l2vpn	read, write		
Examples	The fol	llowing e	example shows how	to attach the pseudowire class to the pseudowire:
	RP/0/F RP/0/F RP/0/F	RSP0/CPU RSP0/CPU RSP0/CPU	0:router(config-1	

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 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	Enters L2VPN configuration mode.
	mpls static label (VPLS), on page 202	Configures the MPLS static labels and the static labels for the access pseudowire configuration.
	neighbor (VPLS), on page 206	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).
	vfi (VPLS), on page 275	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 value		Refresh interval when outbound pseudowire status messages are transmitted.	
			Interval value in seconds. The range is from 1 to 4095. The default value is 30.	
Command Default	None			
Command Modes	L2VPN cor	nfiguration submode		
Command History	Release	Modification		
	Release 4.2.0	This command was introduced.		
Usage Guidelines		iser group assignment is pi	a user group associated with a task group that includes appropriate task reventing you from using a command, contact your AAA administrator	

Task ID	Task Operation ID					
	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)# 12vpn					
	Related Commands	Command	Description			
	pw-class (L2VPN), on page 84	Enters pseudowire class submode to define a pseudowire class template.				

route-target

To specify a route target for the VFI, PBB EVPN or EVPN bridge domain, use the **route-target** command in the BGP autodiscovery mode or in the EVPN EVI BGP configuration mode. To return to the default value, use the **no** form of this command.

route-target {as-number:nn ip-address:nn | [{export | import }] | none} no route-target {as-number:nn ip-address:nn | [{export | import }] | none}

Syntax Description	as-number:n	n Autono	mous system (AS) number of the route distinguisher.
		• as-	-number—16-bit AS number
		Ra	inge for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535.
			the EVPN EVI BGP configuration, range for the 4-byte AS number is 536-4294967295.
		• nn	—32-bit number
	ip-address:n	n IP addr	ess of the route distinguisher.
		• ip-	-address—32-bit IP address
		• nn	—16-bit number
	export	Specifie	es export route target.
	import	aport Specifies import route target.	
	none	Withho	lds BGP RTs.
		Note	This keyword appears only in the EVPN EVI BGP configuration.

I

Command Default	None.				
Command Modes	BGP autodiscovery configuration				
	EVPN EVI BGP configuration				
Command History	Release Modification				
	Release 4.0.0 This command was introduced.				
	Release 4.3.2 Support for this command in the EVPN EVI BGP configuration was introduced.				
Usage Guidelines	To use this command, you must be in a user group associated with a task 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 default value is auto-generated based on VPN-ID.				
	None is used in the EVPN EVI BGP configuration mode to remove the auto-generated route targets. It can only be applied after all other route targets of that type (import or export) have been removed.				
	The Import and Export keywords in the EVPN EVI BGP configuration are optional. If neither is used, both are supported by default.				
Task ID	Task Operations ID				
	l2vpn read, write				
Examples	The following example shows how to configure a bridge domain:				
	<pre>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</pre>				
	The following example shows how to set the BGP route target for the PBB EVPN or EVPN bridge domain:				
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# evpn RP/0/RSP0/CPU0:router(config-evpn)# evi 2 RP/0/RSP0/CPU0:router(config-evpn-evi)# bgp				

RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# route-target 20:30 RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)#

Related Commands	Command	Description
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	Enters L2VPN configuration mode.
	evpn, on page 289	Enters EVPN configuration mode.
	evi, on page 288	Enters the EVPN EVI configuration mode to configure optional BGP settings for a bridge domain or EVI.
	bgp (EVPN), on page 281	Enables BGP in the PBB EVPN configuration.

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 in	nterface.	-
	BVI		Bridge-Group Virtu	al Interface.	-
	BVI interfac	e number	BVI interface numb	er. The range is 1-65535.	-
Command Default	None				
Command Modes	L2VPN bridg	ge-group b	ridge-domain configu	uration submode	
Command History	Release	Modifica	ition	_	
	Release 4.2.0	This com introduce	nmand was ed.	_	
Usage Guidelines		ser group as			task group that includes appropriate task nmand, contact your AAA administrator

L

Task ID Task ID

l2vpn read, write

Operation

The example shows how to specify the L3 bridge domain interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# bridge group bg1
RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bd1
RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# routed interface BVI 100
```

Related Commands	Command	Description	
	dynamic-arp-inspection, on page 53	Validates Address Resolution Protocol (ARP) packets in a network.	
	ip-source-guard, on page 63	Enables source IP address filtering on a layer 2 port.	
	mac (VPLS), on page 196	Enters L2VPN bridge group bridge domain MAC configuration mode.	
	mtu (VPLS), on page 203	Adjusts the maximum packet size or maximum transmission unit (MTU) size for the bridge domain.	
	neighbor (VPLS), on page 206	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).	
	pbb, on page 303	Configures the provider backbone bridge core or edge.	
	shutdown (Bridge Domain), on page 264	Shuts down a bridge domain to bring the bridge and all attachment circuits and pseudowires under it to admin down state.	
	vfi (VPLS), on page 275	Configures virtual forwarding interface (VFI) parameters.	

rpl

To specify one ring port on local node being RPL owner, neighbor or next-neighbor, use the **rpl** command in the Ethernet ring G.8032 instance configuration submode. To disable the port as RPL owner, neighbor or next-neighbor, use the **no** form of this command.

rpl {port0 | port1} {owner | neighbor | next-neighbor} no rpl {port0 | port1} {owner | neighbor | next-neighbor}

Syntax Description	port0	Assigns port0 as RPL owner, neighbor or next-neighbor.
	port1	Assigns port1 as RPL owner, neighbor or next-neighbor.
	owner	Assigns port0 or port1 as RPL owner.

	neighbor		Assigns port0 or port1 as neighbor.		
	next-neighb	or	Assigns port0 or port1 as next neighbor.		
Command Default	None				
Command Modes	Ethernet ring	G.8032 instance configur	ation submode		
Command History	Release	Modification			
	Release 4.1.0	This command was introduced.			
Usage Guidelines		r group assignment is pre	user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator		
Task ID	Task Opera	tion			
	l2vpn read, write				
	This example shows how to assign port0 as neighbor:				
	RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C	200:router(config-l2vp 200:router(config-l2vp 200:router(config-l2vp	<pre>on)# ethernet ring g8032 r1 on-erp)# instance 1 on-erp-instance)# description test on-erp-instance)# profile p1 on-erp-instance)# rpl port0 neighbor</pre>		
Related Commands	Command		Description		
	l2vpn, on pag	e 69	Enters L2VPN configuration mode.		
		g8032, on page 181	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}

Cuntor Decerintian				_	
Syntax Description	brief [Displays brief information on the	he G.8032 ethernet ring.		
	profile Displays information about the G.8032 ethernet ring profile.				
	statistics [statistics Displays the statistics of the G.8032 ethernet ring.			
	status [Displays the status of the G.803	32 ethernet ring.	_	
	summary [Displays a summary of the G.8	032 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 appropria IDs. If the user group assignment is preventing you from using a command, contact your AAA admini for assistance.				
Task ID	Task ID	Operation			
	vlan	read			
	interface	read			
	interface ethernet-ser				
	ethernet-ser		w ethernet ring g8032 con	nmand:	
	ethernet-set	rvices read		nmand:	
	ethernet-set This exampl RP/0/RSP0/ Ethernet r Port0: B A S R Port1: G	rvices read le shows the output of the show CPU0:router# show etherne ing Subring instance 1 is undle-Ether100 (Monitor: PS-Channel: Bundle-Ether1 tatus: RPL, faulty, block emote R-APS NodeId: 0000. igabitEthernet0/0/0/38 (M	t ring g8032 status RPL Owner node in Prot Bundle-Ether100) 00.1 ed 0000.0000, BPR: 0 onitor: GigabitEthernet	tection state	
	ethernet-set This examp RP/0/RSP0/ Ethernet r Port0: B A S Port1: G A S R APS Leve	rvices read le shows the output of the show CPU0:router# show etherne ing Subring instance 1 is undle-Ether100 (Monitor: PS-Channel: Bundle-Ether1 tatus: RPL, faulty, block emote R-APS NodeId: 0000. igabitEthernet0/0/0/38 (M PS-Channel: GigabitEthern tatus: NonRPL emote R-APS NodeId: 0000. 1: 7	t ring g8032 status RPL Owner node in Prot Bundle-Ether100) 00.1 ed 0000.0000, BPR: 0 onitor: GigabitEthernet et0/0/0/38.1	tection state	
	ethernet-sen This exampl RP/0/RSP0/ Ethernet r Port0: B A S Port1: G A Port1: G A S R APS Leve Open APS Profile: WTR in Guard Hold-o	rvices read le shows the output of the show CPU0:router# show etherne ing Subring instance 1 is undle-Ether100 (Monitor: PS-Channel: Bundle-Ether1 tatus: RPL, faulty, block emote R-APS NodeId: 0000. igabitEthernet0/0/0/38 (M PS-Channel: GigabitEthern tatus: NonRPL emote R-APS NodeId: 0000.	t ring g8032 status RPL Owner node in Prot Bundle-Ether100) 00.1 ed 0000.0000, BPR: 0 onitor: GigabitEthernet et0/0/0/38.1 0000.0000, BPR: 0	tection state	

```
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
_____
                                1 Owner
1 Owner
Subring
                                           Protection R,F,B
                               1 Owner
Subring-2
                                           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
                 0
 Pending
                _____
 _____
                2
 Total
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
```

0/0 Never

Tue Mar 15 04:41:00.964 UTC

NR : 3/0

```
Never
       Never
NR, RB : 0/0
                                    0/0
       Never
                                    Never
      Never
                                    Never
     : 19129/0
                                    19129/0
SF
       Wed Mar 16 07:15:28.995 UTC
                                    Wed Mar 16 07:15:28.774 UTC
       Never
                                    Never
     : 0/0
MS
                                    0/0
       Never
                                    Never
       Never
                                    Never
FS
     : 0/0
                                    0/0
                                    Never
       Never
       Never
                                    Never
EVENT : 0/0
                                    0/0
       Never
                                    Never
       Never
                                    Never
             Last entry into state time
State
_____
                                         : Tue Mar 15 04:41:00.933 UTC
Init
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 181	Enables G.8032 ring mode and enters the G.8032 configuration submode.

show I2vpn bridge-domain (VPLS)

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

show l2vpn bridge-domain [{**autodiscovery** | **bd-name** bridge-domain-name | **brief** | **detail** | **group** bridge-domain-group-name | **hardware** | **interface** type interface-path-id | **pw-id** value }] **neighbor IP-address** [{**pw-id** value | **pbb** | **summary**}]

Syntax Description	autodiscovery	(Optional) Displays BGP autodiscovery information.
--------------------	---------------	----------------------------------------------------

I

	bd-name bridge-domain-name	(Optional) Displays filter information on the <i>bridge-domain-name</i> . The <i>bridge-domain-name</i> 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 <i>bridge-domain-group-name</i> 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 pw-id value	(Optional) Displays the bridge domains that contain the pseudowires to match the filter for the neighbor. The <i>ip-address</i> argument is used to specify IP address of the neighbor.						
		(Optional) Displays the filter for the pseudowire ID. The range is from 1 to 4294967295.(Optional) Displays provider backbone bridge information.						
	pbb							
	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.						
	Release 5.1.2	This command was modified to enable filtering the command output for specific pseudowire with just the pseudowire ID.						
	Release 5.3.1	The show command output was enhanced to display VXLAN anycast gateway parameters.						

I

	R	Releas	e									Modif	icatior	1		
	R	Releas	e 5.3.2									enhan	ced to a		l output the MA(
	R	Releas	e 6.1.2									enhan Path F	ced to	display nce and	l output the Ser l Route-]	vice
Usage Guidelines	ap	To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.														
	at	tachn	e interface k nent circuit. wires are dis	In the sa	ample o											
	ps B	seudo GP or	co IOS XR wire with ju LDP signal nd the pseud	st the ps ing (in V	seudowi VPLS),	ire ID.	Howe	ver, in	case of	f config	gurati	ons w	ith BG	P Auto	-discove	ery with
Task ID		ask D	Operations													
	12	2vpn	read													
Examples		his is onfigu	the sample oured:	output fo	or shov	w l2vpi	n brid	ge-doi	nain co	ommane	d wit	h VxL	AN pa	aramete	rs	
	Le	egend ridge Coup MAC MAC MAC MAC MAC MAC MAC MAC MAC Spli Dyna	SP0/CPU0:r : pp = Par group: bg led state: learning: withdraw: C withdraw C withdraw C withdraw ding: oadcast & known unic aging time limit: 400 limit reac port down Secure: di t Horizon mic ARP In ource Guar	tially l, brid disable enabled for Ac sent c relayi Multica ast: en : 300 s), Acti hed: nc flush: sabled, Group: spectic	Progra dge-dom Led d ccess F n: bri ing (ac ast: en habled s, Type ion: nc enable . Loggi none on: dis	ammed. main: 1 PW: end idge po ccess - nabled e: ina cone, No ed ing: d sabled	bgl_b abled oort up to act ctivi (otific lisable , Loge	dl, ic p cess): ty catior ed ging:	disab	state: bled log	-			MSTi:	0	

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 nvel00, Source 1.1.1.1, Multicast Group 225.1.1.1, UDP Port 4789 Anycast VTEP 100.1.1.1, Anycast Multicast Group 224.10.10.1 MAC learning: enabled Flooding: Broadcast & Multicast: enabled Unknown unicast: enabled MAC aging time: 300 s, Type: inactivity MAC limit: 4000, Action: none, Notification: syslog MAC limit reached: no MAC port down flush: enabled MAC Secure: disabled, Logging: disabled

```
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping 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 12vpn 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 VFTs:
   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:
   VFT 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.

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.			

Table 7: show I2vpn bridge-domain Command Field Descriptions

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

RP/0/RSP0/CPU0:router# show 12vpn bridge-domain bd-name bd1

```
Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
List of ACs:
Gi0/1/0/0, state: up, Static MAC addresses: 2, MSTi: 0 (unprotected)
List of Access PWs:
List of VFIs:
VFI 1
Neighbor 10.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
```

The following sample output shows brief information about the bridges:

```
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 I2vpn bridge-domain brief Command Field Descriptions

Field	Description				
Bridge Group/Bridge-Domain Name	Bridge domain group name followed by the bridge domain name are displayed.				
ID	ID assigned to this bridge domain is displayed.				
State	Current state of the bridge domain is displayed.				
Num ACs/up	Total number of attachment circuits that are up in this bridge domain is displayed.				
Num PWs/up	Total number of pseudowires that are up in this bridge domain is displayed. The count includes both VFI pseudowires and access pseudowires.				

The following sample output shows detailed information for IOS-XR releases 5.3.1 and earlier releases.

RP/0/RSP0/CPU0:router# show 12vpn 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:
 VFT 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
                 0x2
       Group ID
                                               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 detailed information for IOS-XR release 5.3.2 release.

```
RP/0/RSP0/CPU0:router# show 12vpn bridge-domain detail
Bridge group: pbb, bridge-domain: pbb core2, id: 11, state: up, ShgId: 0, MSTi: 0
  Coupled state: disabled
  Type: pbb-core
  Number of associated pbb-edge BDs: 1
  EVPN:
   EVI: 2
   Route Distinguisher: (auto) 20.20.20.20:2
   Imposition Statistics:
     Packet Count: 0
     Byte Count : 0
   Disposition Statistics:
     Packet Count: 599123
     Byte Count : 166433410
   AS Number: 200
  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: 12 Filter MAC addresses: P2MP PW: disabled Create time: 03/08/2015 04:09:55 (2w6d ago) No status change since creation ACs: 0 (0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Core, state is up Vlan-id: 2; XC ID 0x80000011 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 Split Horizon Group: none DHCPv4 snooping: disabled IGMP Snooping: enabled IGMP Snooping profile: none MLD Snooping profile: none MMRP Flood Optimization: disabled Storm Control: bridge-domain policer List of EVPNs: EVPN, state: up evi: 2 XC ID 0x80001f51 List of ACs: List of Access PWs: List of VFIs:

The following sample output shows detailed information including P2MP enabled, P-Tree-ID and LSM ID with 1 VFI PW in a bridge domain for IOS-XR 5.3.1 and earlier releases:

RP/0/RSP0/CPU0:router# show 12vpn bridge-domain detail

Bridge group: bg1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4294967295, Action: none, Notification: syslog

MAC limit reached: no MAC port down flush: enabled MAC Secure: disabled, Logging: disabled Split Horizon Group: none Dynamic ARP Inspection: disabled, Logging: disabled IP Source Guard: disabled, Logging: disabled DHCPv4 snooping: disabled IGMP Snooping profile: none Bridge MTU: 1500 MIB cvplsConfigIndex: 1 Filter MAC addresses: Create time: 27/04/2011 10:00:47 (00:14:31 ago) No status change since creation ACs: 0 (0 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up) List of ACs: List of Access PWs: List of VFIs: VFI 1 P2MP: RSVP-TE transport, BGP signaling, PTree ID 14 LSM-ID: 0xdeadbeef PW: neighbor 110.110.110.110, PW ID 1234, state is up (established) PW class not set, XC ID 0xfffc0001 Encapsulation MPLS, protocol LDP Source address 100.100.100.100 PW type Ethernet, control word disabled, interworking none PW backup disable delay 0 sec Sequencing not set PW Status TLV in use MPLS Local Remote 16000 16000 Label Group ID 0x0 0x0 Interface 1 1 MTU 1500 1500 Control word disabled disabled PW type Ethernet Ethernet VCCV CV type 0x2 0x2 (LSP ping verification) (LSP ping verification) VCCV CC type 0x6 0x6 (router alert label) (router alert label) (TTL expiry) (TTL expiry) Incoming Status (PW Status TLV): Status code: 0x0 (Up) in Notification message Outgoing Status (PW Status TLV): Status code: 0x0 (Up) in Notification message MIB cpwVcIndex: 4294705153 Create time: 27/04/2011 10:14:45 (00:00:34 ago) Last time status changed: 27/04/2011 10:15:16 (00:00:02 ago) MAC withdraw message: send 0 receive 0 P2MP-PW: FEC Local Remote Label NULL (inclusive tree) NULL (inclusive tree) P2MP ID 1 1 Flags 0x00 0x00 PTree Type RSVP-TE RSVP-TE 1000 1000 Tunnel ID Ext. Tunnel ID 192.168.0.1 192.168.0.2 P2MP forwarding: enabled Static MAC addresses:

```
Statistics:
    packets: received 0, sent 0
    bytes: received 0, sent 0
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VPN-ID: 1
VFI Statistics:
    drops: illegal VLAN 0, illegal length 0
```

The following sample output shows detailed information including P2MP enabled, P-Tree-ID and LSM ID with 1 VFI PW in a bridge domain for IOS-XR 5.3.2 release:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain detail
Bridge group: bg1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
 MAC learning: enabled
 MAC withdraw: enabled
   MAC withdraw for Access PW: enabled
  Flooding:
   Broadcast & Multicast: enabled
   Unknown unicast: enabled
 MAC aging time: 300 s, Type: inactivity
 MAC limit: 4294967295, Action: none, Notification: syslog
 MAC limit reached: no
 MAC port down flush: enabled
 MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
 Dynamic ARP Inspection: disabled, Logging: disabled
 IP Source Guard: disabled, Logging: disabled
  DHCPv4 snooping: disabled
 IGMP Snooping profile: none
 Bridge MTU: 1500
 MIB cvplsConfigIndex: 1
 Filter MAC addresses:
 Create time: 27/04/2011 10:00:47 (00:14:31 ago)
 No status change since creation
 ACs: 0 (0 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
 List of ACs:
 List of Access PWs:
 List of VFIs:
   VFI 1
      P2MP:
       RSVP-TE transport, BGP signaling, PTree ID 14
       LSM-ID: 0xdeadbeef
      PW: neighbor 110.110.110, PW ID 1234, state is up (established)
       PW class not set, XC ID 0xfffc0001
        Encapsulation MPLS, protocol LDP
       Source address 100.100.100.100
        PW type Ethernet, control word disabled, interworking none
        PW backup disable delay 0 sec
        Sequencing not set
        PW Status TLV in use
         MPLS
                                                      Remote
                      Local
                      16000
                                                      16000
         Label
         Group ID
                      0x0
                                                      0x0
          Interface
                      1
                                                      1
                                                      1500
         MTU
                      1500
         Control word disabled
                                                      disabled
          PW type Ethernet
                                                      Ethernet
         VCCV CV type 0x2
                                                      0 \times 2
```

(LSP ping verification) (LSP ping verification) VCCV CC type 0x6 0x6 (router alert label) (router alert label) (TTL expiry) (TTL expiry) Incoming Status (PW Status TLV): Status code: 0x0 (Up) in Notification message Outgoing Status (PW Status TLV): Status code: 0x0 (Up) in Notification message MIB cpwVcIndex: 4294705153 Create time: 27/04/2011 10:14:45 (00:00:34 ago) Last time status changed: 27/04/2011 10:15:16 (00:00:02 ago) MAC withdraw message: send 0 receive 0 P2MP-PW: FEC Local Remote NULL (inclusive tree) NULL (inclusive tree) Label P2MP ID 0x00 0x00 Flags PTree Type RSVP-TE RSVP-TE Tunnel ID 1000 1000 Ext. Tunnel ID 192.168.0.1 192.168.0.2 P2MP forwarding: enabled Static MAC addresses: Statistics: packets: received 1000 (unicast 1000), sent 0 bytes: received 128000 (unicast 128000), sent 0 MAC move: 10 DHCPv4 snooping: disabled IGMP Snooping profile: none VPN-ID: 1 VFI Statistics: drops: illegal VLAN 0, illegal length 0

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

```
RP/0/RSP0/CPU0:router# show 12vpn bridge-domain detail
Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
  MAC learning: enabled
 MAC withdraw: disabled
 Flooding:
   Broadcast & Multicast: enabled
   Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
 MAC limit reached: yes
  Security: disabled
  DHCPv4 snooping: disabled
 MTU: 1500
  Filter MAC addresses:
 ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
 List of ACs:
   AC: GigabitEthernet0/1/0/0, state is up
      Type Ethernet
      MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
      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 1.1.1.1, PW ID 1, state is up ( established )
       PW class mpls, XC ID 0xff000001
       Encapsulation MPLS, protocol LDP
       PW type Ethernet, control word disabled, interworking none
       PW backup disable delay 0 sec
       Sequencing not set
             MPLS
                          Local
                                                        Remote
         _____
                   16003
         Label
                                                 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, ShqId: 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.

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.

Table 9: show I2vpn bridge-domain detail Command Field Descriptions

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

RP/0/RSP0/CPU0:router# show 12vpn bridge-domain group g1

```
Bridge group: g1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up)
List of ACs:
Gi0/1/0/0, state: up, Static MAC addresses: 2, MSTi: 0 (unprotected)
List of Access PWs:
List of VFIs:
VFI 1
Neighbor 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 display the filter information for the interface on the bridge domain for IOS-XR 5.3.2 release:

RP/0/RSP0/CPU0:router# show 12vpn 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)
Statistics:
packets: received 2000 (multicast 0, broadcast 0, unicast 1000, unknown unicast
1000), sent 1000
bytes: received 93372 (multicast 0, broadcast 0, unicast 64000, unknown unicast
64000), sent 124000
MAC move: 500

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 12vpn 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 that the bridge domain contains the pseudowires to match the filter for the neighbor for IOS-XR 5.3.2 release:

```
RP/0/RSP0/CPU0:router# show 12vpn 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 Access PWs:
List of VFIs:
VFI 1
Neighbor 10.1.1.1 pw-id 1, state: up, Static MAC addresses: 0
Statistics:
```

packets: received 1000 (unicast 1000), sent 0
bytes: received 128000 (unicast 128000), sent 0
MAC move: 10

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

RP/0/RSP0/CPU0:router# show 12vpn 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

The following sample output shows the summary information for the bridge domain including number of bridge-domains with P2MP PW enabled:

RP/0/RSP0/CPU0:router# show 12vpn bridge-domain summary

Number of groups: 1, bridge-domains: 1, Up: 1, Shutdown: 0
Default: 1, pbb-edge: 0, pbb-core: 0
Bridge-domains with P2MP PW enabled: 1
Number of ACs: 3 Up: 3, Down: 0
Number of PWs: 2 Up: 2, Down: 0, Standby: 0

This table describes the significant fields shown in the display.

Table 10: show I2vpn bridge-domain summary Command Field Descriptions

Field	Description
Number of groups	Number of configured bridge domain groups is displayed.
bridge-domains	Number of configured bridge domains is displayed.
Shutdown	Number of bridge domains that are in Shutdown state is displayed.
Number of ACs	Number of attachment circuits that are in Up state and Down state are displayed.
Number of PWs	Number of pseudowires that are in Up state and Down state are displayed. This includes the VFI pseudowire and the access pseudowire.

This example shows sample output of a PBB Edge Bridge Domain for IOS-XR 5.3.1 and earlier releases:

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain bd-name pbb-bd1 detail
Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
Type: pbb-edge, I-SID: 1234
Core-bridge: pbb-bd2
MAC learning: enabled
MAC withdraw: 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
  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
                            888.999.111
        333.444.555
                        Statistics:
       packet totals: receive 3919680, send 9328
       byte totals: receive 305735040, send 15022146
List of ACs:
    AC: GigabitEthernet0/1/0/0, state is up
     Type Ethernet
     MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
     MAC learning: enabled
     Flooding:
       Broadcast & Multicast: enabled
       Unknown unicast: enabled
     MAC aging time: 300 s, Type: inactivity
     MAC limit: 4000, Action: none, Notification: syslog
     MAC limit reached: yes
      Security: disabled
     DHCPv4 snooping: disabled
     Static MAC addresses:
       0000.0000.0000
       0001.0002.0003
      Statistics:
        packet totals: receive 3919680, send 9328
        byte totals: receive 305735040, send 15022146
```

This example shows sample output of a PBB Edge Bridge Domain for IOS-XR 5.3.2 release:

```
RP/0/RSP0/CPU0:router# show 12vpn bridge-domain bd-name pbb-bdl detail
Bridge group: g2, bridge-domain: pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: 0
Type: pbb-edge, I-SID: 1234
Core-bridge: pbb-bd2
MAC learning: enabled
MAC withdraw: 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
```

```
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:
       packets: received 1000 (unicast 1000), sent 0
       bytes: received 128000 (unicast 128000), sent 0
       MAC move: 10
List of ACs:
   AC: GigabitEthernet0/1/0/0, state is up
     Type Ethernet
     MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
     MAC learning: enabled
     Flooding:
       Broadcast & Multicast: enabled
       Unknown unicast: enabled
     MAC aging time: 300 s, Type: inactivity
     MAC limit: 4000, Action: none, Notification: syslog
     MAC limit reached: yes
     Security: disabled
     DHCPv4 snooping: disabled
     Static MAC addresses:
       0000.0000.0000
       0001.0002.0003
     Statistics:
       packets: received 1000 (unicast 1000), sent 0
       bytes: received 128000 (unicast 128000), sent 0
       MAC move: 10
```

This example shows sample output of a PBB Core Bridge Domain:

```
RP/0/RSP0/CPU0:router# show 12vpn bridge-domain bd-name pbb-bd2 detail
Bridge group: g2, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
Type: pbb-core
Number of associated pbb-edge BDs: 1
MAC learning: enabled
MAC withdraw: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: yes
Security: disabled
```

DHCPv4 snooping: disabled MTU: 1500 Filter MAC addresses: ACs: 1 (1 up), 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

The following sample output shows detailed information about a bridge domain that has VXLAN configured.

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain detail
Fri Mar 14 13:30:26.476 EST
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: 10, 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: 14/03/2014 12:37:53 (00:52:33 ago) Last time status changed: 14/03/2014 13:12:20 (00:18:06 ago) ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up) List of ACs: AC: GigabitEthernet0/1/0/8.10, state is up Type VLAN; Num Ranges: 1 VLAN ranges: [10, 10] MTU 1504; XC ID 0x1880017; 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: disabled 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 5010, state is up Encap type VXLAN Overlay nve1, Source 55.55.55.52, Multicast Group 225.0.1.10, UDP Port 8472 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: disabled List of Access PWs: List of VFIs:

The following sample output shows detailed information including bridge-domain VFI configuration for service path preference:

```
RP/0/RSP0/CPU0:router# show 12vpn bridge-domain bd-name bd1 detail
Mon Jun 20 20:03:55.218 EDT
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: bd1, id: 0, state: up, ShgId: 0, MSTi: 0
ACs: 0 (0 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
 List of ACs:
 List of Access PWs:
 List of VFIs:
   VFI v1 (up)
     VPN-ID: 1001, Auto Discovery: BGP, state is Provisioned (Service Connected
     Route Distinguisher: (auto) 1.1.1.1:65524
     Import Route Targets:
                                 1.1.1.1:1001
     Export Route Targets:
                                  1.1.1.1:1001
     Signaling protocol: LDP
     AS Number: 100
     VPLS-ID: (auto) 100:1001
     L2VPN Router ID: 1.1.1.1
     PW: neighbor 2.2.2.2, PW ID 100:1001, state is up ( established )
       PW class not set, XC ID 0 \, \text{xfff8000f}
       Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
       Source address 1.1.1.1
       PW type Ethernet, control word disabled, interworking none
       Sequencing not set
       PW Status TLV in use
                                    MPLS
                                                 Local
                                                                                Remote
           _____ ____
       Incoming Status (PW Status TLV):
         Status code: 0x0 (Up) in Notification message
       MIB cpwVcIndex: 0
       Create time: 20/06/2016 19:40:49 (00:23:06 ago)
       Last time status changed: 20/06/2016 19:40:51 (00:23:04 ago)
       MAC withdraw messages: sent 0, received 0
       Table-policy Name: fwd1
       Forward-class: 1
       Static MAC addresses:
       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
      DHCPv4 snooping: disabled
     IGMP Snooping profile: none
     MLD Snooping profile: none
     VFI Statistics:
       drops: illegal VLAN 0, illegal length 0
```

Related Commands	Command	Description
		Clears the MAC addresses and restarts the bridge domains on the router.

show I2vpn 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|location|private|standby}]

Syntax Description	<i>name</i> 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 <i>ID</i> Instance number about the G.8032 ethernet ring configuration.					
	location Information about the G.8032 ethernet ring configuration for the specified location.					
	private Private information about the G.8032 ethernet ring configuration.					
	standby Standby node specific information					
Command Default	None					
Command Modes	EXEC					
Command History	Release Modification					
	ReleaseThis command was introduced.4.1.0					
	ReleaseThe location and standby keywords were added.4.3.0					
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.					
Task ID	Task Operation ID					
	12vpn 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 12vpn 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 12vpn 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
              : none
    RPL
    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
```

No

No

No

No

No

No

05/18/2010 21:45:57 Create

05/18/2010 21:45:57 Modify

05/18/2010 21:45:57 Resolved

	05/18/2010 21:45:57 Delete	No No				
Related Commands	Command	Description				
	ethernet ring g8032, on page 181	Enables G.8032 ring mode and enters the G.8032 configuration submode.				

show I2vpn forwarding bridge-domain (VPLS)

To display information on the bridge that is used by the forwarding layer, use the **show l2vpn forwarding bridge-domain** command in EXEC mode.

show l2vpn forwarding bridge-domain [*bridge-domain-name*] {**detail**|**hardware** {**egress**|**ingress**}} location *node-id*

Syntax Description	bridge-domain-name	(Optional) Name of a bridge domain.					
	detail	Displays all the detailed information on the attachment circuits and pseudowires.					
	hardware	Displays the hardware location entry.					
	egress	Reads information from the egress PSE.					
	ingress	Reads information from the ingress PSE.					
	location node-id	Displays the bridge-domain information for the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.					
Command Default	None						
Command Modes	EXEC						
Command History	Release Modification						
	Release 3.7.2 This command was introduced.						
	Release 5.3.1 The show command output was enhanced to display VXLAN anycast gateway parameters.						
	Release 5.3.2 The sl	how command output was enhanced to display MAC Move Counter information.					
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate IDs. If the user group assignment is preventing you from using a command, contact your AAA administr for assistance.						
	•••	can display summary information about the number of bridge ports, number of MAC d 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 Operations ID 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 12vpn forwarding bridge-domain location 0/1/CPU0 Bridge-Domain Name ID Ports addr Flooding Learning State g1:bd1 Bridge-domain name: g1:bd1, id: 0, state: up MAC learning: enabled Flooding: Broadcast & Multicast: enabled Unknown unicast: enabled MAC aging time: 300 s, Type: inactivity MAC limit: 4000, Action: none, Notification: syslog MAC limit reached: yes Security: disabled DHCPv4 snooping: profile not known on this node Bridge MTU: 1500 bytes Number of bridge ports: 2 Number of MAC addresses: 65536 Multi-spanning tree instance: 0 GigabitEthernet0/1/0/0, state: oper up Number of MAC: 32770 Sent(Packets/Bytes): 0/21838568 Received (Packets/Bytes): 5704781/444972918 Nbor 1.1.1.1 pw-id 1 Number of MAC: 32766 Sent(Packets/Bytes): 0/0 Received (Packets/Bytes): 5703987/444910986 0 2 65536 Enabled Enabled UP The following sample output shows bridge-domain information for location 0/1/CPU0 for IOS-XR 5.3.2 release: RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain location 0/1/CPU0

```
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
Statistics:
packets: received 5704781 (multicast 0, broadcast 0, unknown unicast 5704781, unicast 0),
sent 0
bytes: received 444972918 (multicast 0, broadcast 0, unknown unicast 444972918, unicast 0),
sent 4950
MAC move: 0
 Nbor 1.1.1.1 pw-id 1
   Number of MAC: 32766
    Sent(Packets/Bytes): 0/0
   Received(Packets/Bytes): 5703987/444910986
                        65536 Enabled Enabled UP
           0
                  2
Statistics:
        packets: received 1000 (unicast 1000), sent 0
        bytes: received 128000 (unicast 128000), sent 0
        MAC move: 10
```

This table describes the significant fields shown in the display:

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.

Table 11: show I2vpn forwarding bridge-domain Command Field Descriptions

This example shows sample output of detailed information on the bridge that is used by the forwarding layer:

RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain detail location 0/0/CPU0 Tue Mar 13 12:35:45.276 PDT Bridge-domain name: bg1:bd1, id: 0, state: up Type: pbb-edge, I-SID: 1000 Core-bridge: bg1:pbb-core1 MAC learning: enabled MAC port down flush: enabled Flooding: Broadcast & Multicast: enabled Unknown unicast: enabled MAC aging time: 300 s, Type: inactivity MAC limit: 4294967295, Action: none, Notification: syslog MAC limit reached: no MAC Secure: disabled, Logging: disabled DHCPv4 snooping: profile not known on this node Dynamic ARP Inspection: disabled, Logging: disabled IP Source Guard: disabled, Logging: disabled IGMP snooping: disabled, flooding: enabled Bridge MTU: 1500 bytes Number of bridge ports: 3 Number of MAC addresses: 0 Multi-spanning tree instance: 0 MIRP-lite: received 0, sent 0

This example shows sample output of detailed information on the bridge that is used by the forwarding layer.

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain detail location 0/1/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 shows detailed information with P2MP PW enabled on the bridge domain:

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain detail location
Tue May 24 23:14:22.934 EDT
Bridge-domain name: bg1:bd1, id: 0, state: up
MAC learning: enabled
MAC port down flush: enabled
Flooding:
  Broadcast & Multicast: enabled
  Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC Secure: disabled, Logging: disabled
DHCPv4 snooping: profile not known on this node
Dynamic ARP Inspection: disabled, Logging: disabled
 IP Source Guard: disabled, Logging: disabled
 IGMP snooping: disabled, flooding: enabled
```

```
Bridge MTU: 1500 bytes
Number of bridge ports: 1
Number of MAC addresses: 0
Multi-spanning tree instance: 0
P2MP PW RSVP-TE enabled, LSM ID: 0x12
GigabitEthernet0/0/0/2.3, state: oper up
Number of MAC: 0
Nbor 2.2.2.2 pw-id 101, state: oper up
Number of MAC: 0
```

The following sample output shows detailed information on a bridge domain for location 0/2/CPU0 that has VXLAN configured.

```
RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain detail location 0/2/CPU0
Bridge-domain name: bg1:10, id: 0, state: up
MAC learning: enabled
MAC port down flush: enabled
Flooding:
   Broadcast & Multicast: enabled
   Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC Secure: disabled, Logging: disabled
 DHCPv4 snooping: profile not known on this node
 Dynamic ARP Inspection: disabled, Logging: disabled
 IP Source Guard: disabled, Logging: disabled
 IGMP snooping: disabled, flooding: enabled
MLD snooping: disabled, flooding: disabled
 Storm control: disabled
 P2MP PW: disabled
Bridge MTU: 1500 bytes
Number of bridge ports: 2
Number of MAC addresses: 0
Multi-spanning tree instance: 0
  GigabitEthernet0/2/0/19.10, 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
    Dynamic arp inspection drop counters:
      packets: 0, bytes: 0
    IP source guard drop counters:
      packets: 0, bytes: 0
 VNI5010, state: oper up
   Number of MAC: 0
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
```

Related Commands	Command	Description		
		Clears the MAC addresses and restarts the bridge domains on the router.		

show I2vpn forwarding bridge-domain mac-address (VPLS)

To display the summary information for the MAC address, use the **show l2vpn forwarding bridge-domain mac-address** command in EXEC mode.

show l2vpn forwarding bridge-domain [bridge-domain-name] **mac-address** {MAC-address | **detail** | **hardware** {**egress** | **ingress**} | **interface** type interface-path-id | **neighbor** address **pw-id** pw-id} location node-id

Syntax Description	bridge-domain-name	(Optional) Name of a bridge domain.					
	MAC-address	MAC address.					
	detail	Displays 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. Displays the match for the pseudowire ID.					
	pw-id pw-id						
	location node-id	Displays the bridge-domain information for the MAC address of the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.					
Command Default	None						
Command Modes	EXEC						
Command History	Release Modif	fication					
	Release 3.7.0 This c	command was introduced.					
	Release 3.7.2 This c	command was introduced.					
	Release 3.8.0 This c	command was introduced.					

Usage Guidelines	To use this comm IDs. If the user go for assistance.									
Fask ID	Task Operatio	ns								
	l2vpn read									
Examples	The following san MAC address:	nple outp	ut shows the	specifie	d locat	ion of th	e bridge-d	lomain name	g1:bd1 fo	or the
	RP/0/RSP0/CPU0	:router#			-	-	domain g	1:bd1 locat	ion 0/1,	CPU0
	Bridge-Domain 1				Ports			g Learning		
	g1:bd1			0				Enabled		
	The following same and summary information				IAC ac	ldresses	that are le	arned on a sp	becified b	ridge
	RP/0/RSP0/CPU0	:router#	show 12vpn	forwa	ding	bridge-	domain m	ac-address	locatio	n 0/1/CPU0
	Fri Mar 14 13: To Resynchron 12vpn resyn	ize MAC †	table from						nd	
	Mac Address	Туре	Learned fr	com/Filt	cered	on L	C learne	d Resync Aç	le	Mapped 1
	0000.0001.0103							0d 0h 2m		N/A
	0000.0001.0104	dynamic	Gi0/1/0/0			0	/1/CPU0	0d 0h 2m	22s	N/A
	0000.0001.0105	dynamic	Gi0/1/0/0			0	/1/CPU0	0d 0h 2m	22s	N/A
	000b.6019.141b	dynamic	Gi0/1/0/8.	10		0	/1/CPU0	Od Oh Om	2s	N/A
	000a.42db.e419	dynamic	nvel			0/1	1/CPU0	0d 0h 0m 23	ls	55.55.55.5
	0013.7faf.681b	dynamic	nvel			0/1	1/CPU0	0d 0h 0m 20	0s	55.55.55.5
	The following sample output shows the MAC address on a specified interface on a specified bridge:									
	RP/0/RSP0/CPU0: 0/1/CPU0	router#	show 12vpn	forwar	ding b	ridge-d	omain g1	:bd1 mac-ad	dress 1.	2.3 locatio
	Mac Address		Learned fr					-		
	0001.0002.0003							N/A		
	The following sat	mple outp	out shows the	hardwa	re info	rmation	from the e	egress pse:		

Mac Address	Туре	Learned from/Filtered on	LC learned	Age
0000.0000.0000	static	Gi0/1/0/0	N/A	N/A
0000.0001.0101	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0102	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0103	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0104	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0105	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0106	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0107	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0108	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0109	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.010a	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.010b	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.010c	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.010d	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.010e	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.010f	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0110	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0111	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0112	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0113	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s
0000.0001.0114	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 24s

The following sample output shows the MAC addresses that are learned on a specified pseudowire on a specified bridge:

RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address neighbor 10.1.1.1 pw-id 1 location 0/1/CPU0

Mac Address	Туре	Learned f:	rom/Filtered on	LC learned	Age	
0000.0003.0101	dynamic	10.1.1.1,	1	0/1/CPU0	0d 01	1 Om 30s
0000.0003.0102	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0103	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0104	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0105	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0106	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0107	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0108	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0109	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.010a	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.010b	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.010c	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.010d	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.010e	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.010f	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0110	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0111	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	om 30s
0000.0003.0112	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0113	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0114	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 30s
0000.0003.0115	dynamic	10.1.1.1,	1	0/1/CPU0	0d Of	1 Om 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:bdl mac-address interface

Mac Address	Туре	Learned from/Filtered on	LC learned	Age
0000.0000.0000	static	Gi0/1/0/0	N/A	N/A
0000.0001.0101	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 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

gigabitEthernet 0/1/0/0 location 0/1/CPU0

The following example shows the list of MAC addresses along with the location details:

RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain mac-address detail location 0/7/CPU0 12fib edm fill mac bag mac info 0 12fm 13 encap vlan=0 12fib get mac 13 encap vlan str 12fib edm fill mac bag mac info 0 12fm 13 encap vlan=0 l2fib_get_mac_l3_encap_vlan_str Bridge-domain name: bg1:bd1, id: 0, state: up MAC learning: enabled MAC port down flush: enabled Flooding: Broadcast & Multicast: enabled Unknown unicast: enabled MAC aging time: 300 s, Type: inactivity MAC limit: 4000, Action: none, Notification: syslog MAC limit reached: no MAC Secure: disabled, Logging: disabled DHCPv4 snooping: profile not known on this node Dynamic ARP Inspection: disabled, Logging: disabled IP Source Guard: disabled, Logging: disabled IGMP snooping: disabled, flooding: enabled Routed interface: BVI100, Xconnect id: 0xfff00001, state: up IRB platform data: {0x0, 0x0, 0x0, 0x0}, len: 4 Bridge MTU: 1500 bytes Number of bridge ports: 1 Number of MAC addresses: 2 Multi-spanning tree instance: 0 Mac Address: 029d.af84.4105, LC learned: N/A Age: N/A, Flag: static, BVI L3 encapsulation Vlan = 0GigabitEthernet0/0/0/0.1, state: oper up Number of MAC: 1 Mac Address: 0000.0002.0003, LC learned: N/A Age: N/A, Flag: static

L3 encapsulation Vlan = 1001

RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain mac-address location 0/1/CPU0

Mac Address	Туре	Learned from/Filtered on	LC learned	Age
0000.0000.0000	static	Gi0/1/0/0	N/A	N/A
0000.0001.0101	dynamic	Gi0/1/0/0	0/1/CPU0	0d 0h 2m 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

This example shows sample output of the **show l2vpn forwarding bridge-domain mac-address location** command:

RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain mac-address location 0/1/CPU0 Mac Address Type Learned from/Filtered on LC learned Age Mapped to _____ 0002.0003.0004 filter bg1:bd1 N/A N/A 0002.0003.0005 filter bg1:bd1 N/A N/A 0002.0003.0006 filter bg1:bd1 N/A N/A 0002.0002.0002 static Gi0/0/0.1 N/A N/A 0333.0444.0555 static bg1:bd2 N/A N/A 0777.0888.0999 0444.0555.0666 static bg1:bd2 N/A N/A 0888.0999.0111

This example shows sample output of the **show l2vpn forwarding bridge-domain mac-address detail location** command:

RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mac-address detail location
0/1/CPU0

```
Bridge-domain name: bg1:bd1, id: 0, 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: 4294967295, 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: 2
```

```
Number of MAC addresses: 1
Multi-spanning tree instance: 0
PBB Edge, state: up
Number of MAC: 1
Mac Address: 0004.0005.0006, LC learned: N/A,
Mapping value: 0007.0008.0009
Age: N/A, Flag: mapping
```

Related Commands	Command	Description	
	show I2vpn forwarding bridge-domain (VPLS), on page 247	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 O	G.8032 ethernet ring configuration.	
	instanceID	Instance number about the G.8	032 ethernet ring configuration.	
	location	Location specified in the rack/s	slot/module notation.	
	private	Private information about the C	6.8032 ethernet ring configuration.	
Command Default	None			
Command Modes	EXEC			
Command History	Release	Modification	_	
	Release 4.1.0	This command was introduced.	-	
Usage Guidelines		ser group assignment is preventi	group associated with a task group t ng you from using a command, con	
Task ID	Task Ope ID	ration		
	l2vpn read	1		

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
    RPI.
             : 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 12vpn 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
```

-	GigabitEtherne GigabitEtherne			d
ethernet rin	ng g8032 instar	ce trace his	story [Num ever	ts:
Time	Event		Sticky	 Mar
====	=====		======	===
05/18/2010 2	21:45:54 Create	!	No	No
05/18/2010 2	21:45:57 Create	!	No	No
0E/10/0010 /	21:45:57 Modify	,	No	No
UD/10/2010 2				

Related Commands	Command	Description		
	ethernet ring g8032, on page 181	Enables G.8032 ring mode and enters the G.8032 configuration submode.		

show I2vpn 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.

Syntax Description	interface n	ame	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		user group assignment is preve	er group associated with a task group that includes appropriate task nting you from using a command, contact your AAA administrator

show l2vpn forwarding protection main-interface [interface name] [{detail | location | private}]

Task ID

Task Operation ID

l2vpn read

Example

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

GigabitEthernet0/0/0/0	1	forwar	d	
GigabitEthernet0/0/0/0	2	forwar	d	
GigabitEthernet0/0/0/1	1	forwar	d	
<pre># show l2vpn forwarding prot</pre>				n <r i="" s=""></r>
Main Interface ID	Insta	ince 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 prot	ection mai	n-interface	private locatio	on <r i<="" s="" td=""></r>
Main Interface ID	Insta	ince State	# of subIntf	
GigabitEthernet0/0/0/0	1	forward	1	

Related Commands	Command	Description
	l2vpn, on page 69	Enters L2VPN configuration mode.

show I2vpn 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 | location | private
| standby}]

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				tion in detail about the G.8032 ethernet figuration.	
	location			Location specific information		
	private	Private information about the G.8032 ethernet rin configuration.				
	standby		Standby node specific information.			
Command Default	None					
Command Modes	EXEC					
Command History	Release	Modification				
	Release 4.1.0	This command w	as introduced.			
	Release 4.3.0	The keywords loc	eation and standby wer	e added.		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate ta IDs. If the user group assignment is preventing you from using a command, contact your AAA administrat for assistance.					
Task ID	Task Ope ID	eration				
	l2vpn rea	d				
	-					
	Example					
	-	le shows the output	from the show l2vpn g	protection r	nain-interface command:	
	This examp		from the show l2vpn p 2vpn protection main			
	This examp RP/0/0/CPU Main Inter	JO:router# show l2		n-interfac Protected	Blocked	
	This examp RP/0/0/CPU Main Inter GigabitEth Instanc Stat Sub- Flus	J0:router# show 12 rface ID hernet0/0/0/0 ce : 0 ce : FORWA -Intf # : 1 sh # : 0	2vpn protection main Subintf Count 2 1	n-interfac Protected 	Blocked	
	This examp RP/0/0/CPU Main Inter GigabitEth Instanc Stat Sub- Flus Sub Main Inter	J0:router# show 12 rface ID hernet0/0/0/0 ce : 0 ce : FORW2 -Intf # : 1 sh # : 0 p-interfaces : Gig rface ID	2vpn protection main Subintf Count 1 1 ARDING	n-interfac Protected None D.4 Protected	Blocked No Blocked	

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

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

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

RP/0/RSP0/CPU0:router# show 12vpn protection main-interface detail

Main Interface ID	<pre># of subIntf</pre>	
GigabitEthernet0/1/0/19		No
Main Interface ID	# of subIntf	
GigabitEthernet0/1/0/20	3	No
Main Interface ID	# of subIntf	
GigabitEthernet0/1/0/3		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 12vpn protection main-interface private

Main Interface ID	Ref Count	Protected	Blocked	If Handle	Registered
GigabitEthernet0/0/0/0	3	None	No	0x20000020	No
<pre>Instance : 0 State : FO Sub-Intf # : 0 Bridge D # : 0 Flush # : 0 Sub-interfaces : Gi Instance event trace</pre>	gabitEthernet0/C	Ack # : N-Ack # : Rcv # : 0/0/0.4	0 0 0	8]	
	Update L2FIB		State ======= Invalid FORWARD T FORWARD	= == 13 ING 0	tion ====== 4833160

Related Commands	Command	Description	
	l2vpn, on page 69	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.

	To re-enable i	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, th	e bridge is not shutdown		
Command Modes	L2VPN bridg	e group bridge domain co	onfiguration	
Command History	Release	Modification		
	Release 3.7.2	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 ta IDs. If the user group assignment is preventing you from using a command, contact your AAA administrat for assistance.			
	-		VFIs associated with the bridge domain are disabled. You can still e bridge domain as well as the VFIs associated with the bridge domain.	
Task ID	Task Opera ID	tions		
	l2vpn read, write			
Examples	The following	g example shows how to	disable the bridge domain named bar:	
	RP/0/RSP0/C RP/0/RSP0/C RP/0/RSP0/C	PU0:router# configure PU0:router(config)# 1 PU0:router(config-12v PU0:router(config-12v PU0:router(config-12v	pn) # bridge group 1 pn-bg) # bridge-domain bar	
Related Commands	Command		Description	
	bridge-doma	in (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.	
	bridge group	(VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.	
	l2vpn, on pag	je 69	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 shutdownSyntax DescriptionThis command has no keywords or arguments.Command DefaultBy default, the VFI is not shutdown.Command ModesL2VPN bridge group bridge domain VFI configurationCommand HistoryRelease Modification
Release 3.7.2 This command was

introduced.

Usage Guidelines To

To use this command, you must be in a user group associated with a task group that includes appropriate 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 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	Enters L2VPN configuration mode.
	mpls static label (VPLS), on page 202	Configures the MPLS static labels and the static labels for the access pseudowire configuration.

I

Command	Description
neighbor (VPLS), on page 206	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 or in the L2VPN bridge group bridge domain VFI multicast P2MP configuration 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	bg Enables BGP protocol signaling.
	h p Enables LDP protocol signaling.
Command Default	LDP signaling is enabled.
Command Modes	BGP autodiscovery configuration
	L2VPN bridge group bridge domain VFI multicast P2MP configuration
Command History	Release Modification
	Release 3.9.1 This command was introduced.
	Release 5.1 Support for this command in the L2VPN bridge group bridge domain VFI multicast P2MP configuration mode was introduced.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
Task ID	Task Operations ID
	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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group EGroup RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain eastdomain RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# vfi eastvfi RP/0/RSP0/CPU0:router(config-12vpn-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 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	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 Operations ID		
	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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group metroA RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain east RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain east RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# interface GigabitEthernet0/1/0/6.15 RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-ac)# split-horizon group RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-ac)# commit Related Commands Command Description

show I2vpn bridge-domain (VPLS), on page 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-addre	ess Static MAC address that is u	sed to filter on the bridge domain.	
	drop	Drops all traffic that is goin	g to the configured MAC address.	
Command Default	No static M	IAC address is configured.		
Command Modes	L2VPN bri	dge group bridge domain MAC	configuration	
Command History	Release	Modification		
	Release 3.	7.2 This command was introduced.		
Usage Guidelines		user group assignment is preven	r group associated with a task group ating you from using a command, con	
Task ID	Task Ope ID	erations		
	l2vpn rea wr			

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 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	Enters L2VPN configuration mode.
	mac (VPLS), on page 196	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 M	IAC 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 cor	nmand, you must be in a use	r group associated with a task

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

I

Task ID	Task Operations ID				
	l2vpn read,				
	write				
Examples	The following example shows how to associate a remote MAC address with a pseudowire:				
	<pre>RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group 1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# vfi model RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000 RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-vfi-pw)# static-mac-address 1.1.1</pre>				
	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)# 12vpn RP/0/RSP0/CPU0:router (config-12vpn)# bridge group 1 RP/0/RSP0/CPU0:router (config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router (config-12vpn-bg-bd)# interface GigabitEthernet 0/1/0/0 RP/0/RSP0/CPU0:router (config-12vpn-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:				
Related Commands	Command	Description			
	bridge-domain (VPLS), on pag	e 176 Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.			
	bridge group (VPLS), on page	177 Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.			
	l2vpn, on page 69	Enters L2VPN configuration mode.			
	mpls static label (VPLS), on pa	Ige 202 Configures the MPLS static labels and the static labels for the access pseudowire configuration.			
	neighbor (VPLS), on page 206	Adds an access pseudowire port to a bridge domain or a pseudowire to a bridge virtual forwarding interface (VFI).			
	vfi (VPLS), on page 275	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 con	figuration submode	
Command Modes		ingulation submode	
Command History	Release	Modification	
	Release 4.1.0	This command was introduced.	
Usage Guidelines		ser group assignment is pre	user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator
Task ID	Task Ope ID	ration	
	l2vpn read writ		
	This examp	le shows how to enable the	G.8032 ring mode:
	RP/0/RSP0/ RP/0/RSP0/	CPU0:router# configure CPU0:router(config)# 12x CPU0:router(config-12vg CPU0:router(config-12vg	on-erp)# tcn-propagation
Related Commands	Command		Description
	ethernet rir	ng g8032, on page 181	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

	<i>seconds</i> 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 bridg	e group bridge domain N	MAC aging configuration		
Command History	Release	Modification			
	Release 3.7.2	This command was introduced.			
Usage Guidelines		er group assignment is pr	a user group associated with a task group that includes appropriate task reventing you from using a command, contact your AAA administrator		
			AC address for the duration of the maximum aging time, the dynamic oved from the forwarding table.		
Task ID	Task Opera ID	tions			
	l2vpn read, write				
Examples	write The following	g example shows how to	increase the maximum aging time to 600 seconds. After 600 lress, the MAC address is removed form the forwarding table.		
Examples	write The following seconds of ina RP/0/RSP0/CH RP/0/RSP0/CH RP/0/RSP0/CH RP/0/RSP0/CH RP/0/RSP0/CH	g example shows how to activity from a MAC add 200:router# configure 200:router(config)# 1 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x	Iress, the MAC address is removed form the forwarding table. L2vpn rpn) # bridge group 1 rpn-bg) # bridge-domain bar		
	write The following seconds of ina RP/0/RSP0/CH RP/0/RSP0/CH RP/0/RSP0/CH RP/0/RSP0/CH RP/0/RSP0/CH	g example shows how to activity from a MAC add 200:router# configure 200:router(config)# 1 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x	<pre>lress, the MAC address is removed form the forwarding table. l2vpn zpn) # bridge group 1 zpn-bg) # bridge-domain bar zpn-bg-bd) # mac zpn-bg-bd-mac) # aging zpn-bg-bd-mac-aging) # time 600</pre>		
	write The following seconds of ina RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI	g example shows how to activity from a MAC add 200:router# configure 200:router(config)# 1 200:router(config-12v 200:router(config-12v 200:router(config-12v 200:router(config-12v	Iress, the MAC address is removed form the forwarding table. L2vpn rpn) # bridge group 1 rpn-bg) # bridge-domain bar rpn-bg-bd) # mac rpn-bg-bd-mac) # aging		
	write The following seconds of ina RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI Command aging (VPLS),	g example shows how to activity from a MAC add 200:router# configure 200:router(config)# 1 200:router(config-12v 200:router(config-12v 200:router(config-12v 200:router(config-12v	Iress, the MAC address is removed form the forwarding table. L2vpn zpn) # bridge group 1 zpn-bg) # bridge-domain bar zpn-bg-bd) # mac zpn-bg-bd-mac) # aging zpn-bg-bd-mac-aging) # time 600 Description Enters the MAC aging configuration submode to set the aging		
	write The following seconds of ina RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI BP/0/RSP0/CI Command aging (VPLS), bridge-domain	g example shows how to activity from a MAC add 200:router# configure 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x	Iress, the MAC address is removed form the forwarding table. L2vpn rpn) # bridge group 1 rpn-bg) # bridge-domain bar rpn-bg-bd) # mac rpn-bg-bd-mac) # aging rpn-bg-bd-mac-aging) # time 600 Description Enters the MAC aging configuration submode to set the aging parameters such as time and type. Establishes a bridge domain, and enters L2VPN bridge group bridge		
	write The following seconds of ina RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI BP/0/RSP0/CI Command aging (VPLS), bridge-domain	g example shows how to activity from a MAC add 200:router# configure 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-12x 200:router(config-1	<pre>Iress, the MAC address is removed form the forwarding table. L2vpn rpn) # bridge group 1 rpn-bg) # bridge-domain bar rpn-bg-bd) # mac rpn-bg-bd-mac) # aging rpn-bg-bd-mac-aging) # time 600 Description Enters the MAC aging configuration submode to set the aging parameters such as time and type. Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode. Creates a bridge group so that it can contain bridge domains and</pre>		
Examples Related Commands	write The following seconds of ina RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI RP/0/RSP0/CI Distance Command aging (VPLS), bridge-domain bridge group	g example shows how to activity from a MAC add 200:router# configure 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=12x 200:router(config=1	Iress, the MAC address is removed form the forwarding table. L2vpn rpn)# bridge group 1 rpn-bg)# bridge-domain bar rpn-bg-bd)# mac rpn-bg-bd-mac)# aging rpn-bg-bd-mac-aging)# time 600 Description Enters the MAC aging configuration submode to set the aging parameters such as time and type. Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode. Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.		

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
	ReleaseThis command was5.1introduced.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
Task ID	Task Operation ID
	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)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group 1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# vfi v1 RP/0/RSP0/CPU0:router(config-12vpn-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
	Configures point to multi-point pseudowire in a VFI.

Command	Description
vfi (VPLS), on page 275	Configures virtual forwarding interface (VFI) parameters.
bridge-domain (VPLS), on page 176	Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
12vpn, on page 69	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.

	no type {at	osolute inactivity}	
Syntax Description	absolute Co	onfigures the absolute aging type.	-
	inactivity Co	onfigures the inactivity aging type.	-
Command Default	By default, th	e inactivity type is configured.	
Command Modes	L2VPN bridg	e group bridge domain MAC ag	ing configuration
Command History	Release	Modification	
	Release 3.7.2	2 This command was introduced.	
Usage Guidelines		er group assignment is preventin	oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
	In general, the	e type is set to inactivity. With an	inactivity type configuration, a MAC address is removed from

type {absolute | inactivity}

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		owing example shows how to of the bridge domain named b	configure the MAC address aging type to absolute for every par:
	RP/0/RS RP/0/RS RP/0/RS		2vpn pn)# bridge group 1 pn-bg)# bridge-domain bar
	RP/0/RS	SPO/CPU0:router(config-l2v SPO/CPU0:router(config-l2v SPO/CPU0:router(config-l2v	
Related Commands	RP/0/RS	SPO/CPU0:router(config-l2v SPO/CPU0:router(config-l2v	pn-bg-bd-mac)# aging
Related Commands	RP/0/RS RP/0/RS Comma	SPO/CPU0:router(config-l2v SPO/CPU0:router(config-l2v	pn-bg-bd-mac)# aging pn-bg-bd-mac-aging)# type absolute
Related Commands	RP/0/RS RP/0/RS Comma aging (SPO/CPU0:router(config-12v SPO/CPU0:router(config-12v	pn-bg-bd-mac) # aging pn-bg-bd-mac-aging) # type absolute Description Enters the MAC aging configuration submode to set the aging
Related Commands	RP/0/RS RP/0/RS Comma aging (' bridge-	SPO/CPU0:router(config-12v SPO/CPU0:router(config-12v and VPLS), on page 172	pn-bg-bd-mac) # aging pn-bg-bd-mac-aging) # type absolute Description Enters the MAC aging configuration submode to set the aging parameters such as time and type. Establishes a bridge domain, and enters L2VPN bridge group bridge
Related Commands	RP/0/RS RP/0/RS aging (' bridge- bridge	SPO/CPU0:router(config-12v SPO/CPU0:router(config-12v Ind VPLS), on page 172 domain (VPLS), on page 176	pn-bg-bd-mac) # aging pn-bg-bd-mac-aging) # type absolute Description Enters the MAC aging configuration submode to set the aging parameters such as time and type. Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode. Creates a bridge group so that it can contain bridge domains and
Related Commands	RP/0/RS RP/0/RS Comma aging (' bridge- bridge l2vpn, c	SPO/CPU0:router(config-12v SPO/CPU0:router(config-12v Ind VPLS), on page 172 domain (VPLS), on page 176 group (VPLS), on page 177	pn-bg-bd-mac) # aging pn-bg-bd-mac-aging) # type absolute Description Enters the MAC aging configuration submode to set the aging parameters such as time and type. Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode. Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.

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.

	no vfi vfi-name
Syntax Description	<i>vfi-name</i> Name of the specified virtual forwarding interface.
Command Default	None
Command Modes	L2VPN bridge group bridge domain configuration

vfi vfi-name

Command History	Release	Modification	
	Release	3.7.2 This command wa introduced.	15
Usage Guidelines		e user group assignment	e in a user group associated with a task group that includes appropriate task is preventing you from using a command, contact your AAA administrator
	Use the v	fi command to enter L2	VPN bridge group bridge domain VFI configuration mode.
Task ID	Task (ID	Operations	
	l2vpn r	ead, vrite	
Examples	The follo	wing example shows ho	w to create a VFI:
	RP/0/RSE RP/0/RSE RP/0/RSE RP/0/RSE	20/CPU0:router(config	<pre>i # 12vpn i = 12vpn)# bridge group 1 i = 12vpn-bg)# bridge-domain bar i = 12vpn-bg-bd)# vfi v1</pre>
Related Commands	Comman	ıd	Description
	bridge-d	omain (VPLS), on page 1	76 Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge g	roup (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, or	n page 69	Enters L2VPN configuration mode.
	mpls sta	tic label (VPLS), on page	202 Configures the MPLS static labels and the static labels for the access pseudowire configuration.
	neighbo	r (VPLS), on page 206	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	g of MAC withdraw messages to access pseudowires.		
	disable	Disables MAC addr	ess withdrawal.		
Command Default	By default, MA	C address withdrawal is	s enabled.		
Command Modes	L2VPN bridge group bridge domain MAC configuration				
Command History	Release	Modification			
	Release 3.7.2	This command was intro	oduced.		
	Release 4.0.0	The access-pw disable	keyword was added.		
Usage Guidelines			user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator		
Task ID	Task Operatio	ons			
	l2vpn read, write				
Examples	The following e	example shows how to e	nable disable MAC withdrawal:		
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# 12vpn RP/0/RSP0/CPU0:router(config-12vpn)# bridge group 1 RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bar RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# mac RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-mac)# withdraw disable				
			lisable sending MAC withdrawal messages to access		
	RP/0/RSP0/CPU RP/0/RSP0/CPU RP/0/RSP0/CPU RP/0/RSP0/CPU	0:router(config-l2vp	on)# bridge group 1 on-bg)# bridge-domain bar		
Related Commands	Command		Description		
	bridge-domain	(VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.		
	bridge group (\	/PLS), on page 177	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 69	Enters L2VPN configuration mode.
mac (VPLS), on page 196	Enters L2VPN bridge group bridge domain MAC configuration mode.



Provider Backbone Bridge Commands

The IEEE 802.1ah standard (Ref [4]) provides a means for interconnecting multiple provider bridged networks inorder to build a large scale end-to-end Layer 2 provider bridged network.

For detailed information about PBB concepts, configuration tasks, and examples, see the L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers.

- backbone-source-mac, on page 280
- bgp (EVPN), on page 281
- clear mmrp-flood-optimization statistics, on page 283
- clear l2vpn forwarding counters bridge-domain mmrp location, on page 283
- debug mmrp-flood-optimization packets, on page 284
- debug mmrp-flood-optimization protocol, on page 285
- ethernet-segment, on page 286
- ethernet-segment (evpn), on page 287
- evi, on page 288
- evpn, on page 289
- evpn evi, on page 290
- flushagain, on page 291
- flood-time, on page 292
- force single-homed, on page 293
- identifier, on page 294
- join-time (PBB), on page 295
- interface (EVPN), on page 296
- leaveall-time (PBB), on page 297
- leave-time (PBB), on page 298
- load-balancing-mode, on page 299
- mmrp-flood-optimization, on page 300
- mac-flush mvrp, on page 301
- mode singleton, on page 302
- pbb, on page 303
- peering, on page 304
- periodic transmit (PBB), on page 305
- programming, on page 306
- recovery, on page 307
- rewrite ingress tag push, on page 309

- service-carving, on page 310
- show evpn ethernet-segment, on page 311
- show evpn evi, on page 314
- show evpn summary, on page 317
- show l2vpn bridge-domain pbb, on page 318
- show l2vpn forwarding bridge pbb, on page 325
- show l2vpn forwarding pbb backbone-source-mac, on page 327
- show l2vpn pbb backbone-source-mac, on page 328
- show mmrp-flood-optimization, on page 328
- static-mac-address, on page 330
- timers, on page 332
- unknown-unicast-bmac, on page 333

backbone-source-mac

To configure the backbone source MAC address, use the **backbone-source-mac** command in pbb configuration mode or in the EVPN Interface Ethernet segment configuration mode. To return to the default behavior, use the **no** form of this command.

Note	If the backbone source MAC address is not configured then one of the reserved addresses from the Chassi MAC pool is chosen automatically. To view the reserved address, use the show l2vpn pbb backbone-source-mac command.
	backbone-source-mac mac-address no backbone-source-mac mac-address
Syntax Description	mac address Backbone source MAC address in hexadecimal format.
Command Default	None
Command Modes	PBB configuration EVPN Interface Ethernet segment configuration
Command History	Release Modification
	Release 3.9.1 This command was introduced.
	Release 4.3.2 Support for this command in the EVPN Interface Ethernet segment configuration was introduced.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate ta IDs. If the user group assignment is preventing you from using a command, contact your AAA administrat for assistance.

The command default in the EVPN Interface Ethernet segment configuration is the CE system-id with administrative bit flip. Use this command to overwrite the CE-system id of an Ethernet Segment. The backbone source MAC can be configured only on a bundle interface.

Task ID	Task Operations ID						
	l2vpn read, write						
Examples	In the following example, the backt	pone source MAC address is set to 0045.1200.04:					
	config l2vpn pbb backbone-source-mac 0045.1200.0400 !						
	This example shows how to set the backbone source MAC address in the EVPN Interface Ethernet segment configuration mode:						
	RP/0/RSP0/CPU0:router(config-e	<pre>evpn evpn)# interface bundle-ether 1 evpn-ac)# ethernet segment evpn-ac-es)# backbone-source-mac 0045.1200.0400</pre>					
Related Commands	Command	Description					
	pbb, on page 303	Configures the provider backbone bridge core or edge.					
	evpn, on page 289	Enters EVPN configuration mode.					
	interface (EVPN), on page 296	Enters the EVPN Interface configuration mode.					

bgp (EVPN)

To enable Border Gateway Protocol (BGP) in the PBB EVPN configuration, use the **bgp** command in the EVPN configuration or EVPN EVI configuration mode. To disable the BGP configuration, use the **no** form of this command.

Enters EVPN interface ethernet segment configuration mode.

```
bgp [rd]
bgp [{rd | route-target }]
no bgp
```

ethernet-segment, on page 286

I

Syntax Description	rd	Sets the Route Distinguisher.				
	route-targ	et Sets the Route Target				
Command Default	None.					
Command Modes	EVPN conf	iguration				
	EVPN EVI	configuration				
Command History	Release	Modification				
	Release 4.3.2	This command was introduced.				
Usage Guidelines		ser group assignment is	n a user group associated with a task group that includes appropriate task preventing you from using a command, contact your AAA administrator			
	The keywor	rd route-target is suppor	ted only in the EVPN EVI BGP configuration.			
Task ID	Task Ope ID	eration				
	l2vpn read wri					
	This example shows how to enable BGP in the EVPN configuration mode:					
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# evpn RP/0/RSP0/CPU0:router(config-evpn)# bgp RP/0/RSP0/CPU0:router(config-evpn-bgp)#					
	This example shows how to enable BGP in the EVPN EVI configuration mode:					
	RP/0/RSP0/ RP/0/RSP0/ RP/0/RSP0/	CPU0:router# configu CPU0:router(config)# CPU0:router(config-e CPU0:router(config-e CPU0:router(config-e	evpn vpn)# evi 2 vpn-evi)# bgp			
Related Commands	Command		Description			
	evpn, on pa	age 289	Enters EVPN configuration mode.			
	evi, on pag	e 288	Enters the EVPN EVI configuration mode to configure optional BGP settings for a bridge domain or EVI.			
	route-targe	et, on page 216	Specifies a route target for the VFI, PBB EVPN or EVPN bridge domain.			

rd

L

clear mmrp-flood-optimization statistics

To clear the stored MRP protocol statistics on all the pseudowires or a specific pseudowire, use the **clear mmrp-flood-optimization statistics** command in the EXEC mode.

clear mmrp-flood-optimization statistics {all | pw pw-ID neighbor}

Syntax Description	all		Clear the stored MRP protocol statistics on all the pseudowires
	pw		Indicates a specific pseudowire
	neighbor		Indicates the IP address of the neighbor.
	pw-id		Indicates the pseudowire ID.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	-
	Release 5.1.2	This command was introduced	_
Usage Guidelines		ser group assignment is preventing	roup associated with a task group that includes appropriate and you from using a command, contact your AAA administration
Task ID	Task ID	Operation	

RP/0/RSP0/CPU0:router#clear mmrp-flood-optimization statistics all

clear I2vpn forwarding counters bridge-domain mmrp location

To clear the MMRP flood statistics on a given bridge-domain on a specified location, use the **clear l2vpn** forwarding counters bridge-domain mmrp location command in the EXEC command.

clear l2vpn forwarding counters bridge-domain mmrp location location

Syntax Description *location* Specifies the location in rack/slot/module notation.

Command Default	None					
Command Modes	EXEC					
Command History	Release	Modification				
	Release 5.1.2	This command w	vas introduced.			
Usage Guidelines		ser group assignme			ncludes appropriate tas your AAA administrate	
Task ID	Task ID	Operation				
	ethernet-serv	vices read, write				

The following command shows how to clear the mmrp flood statistics on a given bridge-domain on a specified location:

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

debug mmrp-flood-optimization packets

To debug the flood optimization for PBB VPLS feature at the packet level, use the **debug mmrp-flood-optimization packets** command in the EXEC mode.

debug mmrp-flood-optimization packets {**brief** | **full** | **hexdump**} [**direction** {**received** | **sent**}] [**pw** *neighbor pw-id*]

Syntax Description	brief	Brief packet debug.	
	full	Full packet debug.	
	hexdump	Raw packet output.	
	direction	Restricts output to a packet direction.	
	received	Packets received.	
	sent	Packets sent.	
	pw	Specifies a pseudowire to filter.	
	neighbor	IP address of the neighbor	
	pw-id	Pseudowire ID.	

Command Default None

Command Modes	EXEC			
Command History	Release	Modification		
	Release 5.1.2	This command	was introduced.	
Usage Guidelines		iser group assignm	-	oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task ID	Operation		
	ethernet-ser	rvices read, write		

The following command shows how to use the debug mmrp-flood-optimization packets command:

RP/0/RSP0/CPU0:router#debug mmrp-flood-optimization packets brief

debug mmrp-flood-optimization protocol

To debug the flood optimization for PBB VPLS feature at the protocol level, use the **debug mmrp-flood-optimization protocol** command in the EXEC mode.

debug mmrp-flood-optimization protocol [isid isid]

Syntax Description	isid Speci	fies the service instance identif	er.
	isid Servi	ce instance identifier.	
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 5.1.2	This command was introduce	d.
Usage Guidelines		ser group assignment is preven	group associated with a task group that includes appropriate task ing you from using a command, contact your AAA administrator
Task ID	Task ID	Operation	
	ethernet-serv	vices read, write	

The following command shows how to use the debug mmrp-flood-optimization protocol command:

RP/0/RSP0/CPU0:router#debug mmrp-flood-optimization protocol isid 3

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	backb	backbone-source-mac Specifies Backbone Source MAC.			
	identif	identifier Specifies Ethernet		Segment Identifier.	
	load-b	alancing-mode	e Specifies load bala	ancing mode.	
	service	e-carving	Specifies service ca	rving.	
Command Default	None.				
Command Modes	EVPN	interface config	uration		
Command History	Releas	e Modifica	ation		
	Releas 4.3.2	e This con	nmand was introduced.		
Usage Guidelines		the user group a	Ŭ	1	h a task group that includes appropriate task command, contact your AAA administrator
Task ID	Task ID	Operation			
	l2vpn	read, write			
	This ex	ample shows ho	ow to enter the EVPN in	nterface ethernet se	egment configuration mode:
	RP/0/R	SP0/CPU0:rout	er# configure		

```
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)#

Related	Commands
---------	----------

ommands	Command	Description						
	interface (EVPN), on page 296	Enters the EVPN Interface configuration mode.						
	backbone-source-mac, on page 280	Configures the backbone source MAC address.						
	load-balancing-mode, on page 299	Sets the load balancing mode of a physical port or bundle to active-active.						

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 S	pecifies LACP ESI-auto-generation for ESI type 1.
	auto-generation-disable D	isables ESI auto-generation.
Command Default	By default, EVPN auto-gener	rates an ESI value for the bundle interfaces by retrieving LACP information.
Command Modes	EVPN configuration mode	
Command History	Release Modification	
	ReleaseThis command6.3.2	was introduced.
Usage Guidelines	This command allows mLAC	P to decide to either forward or stop EVPN multipath resolution on remote ESI.
Task ID	Task Operation ID	
	l2vpn read, write	
	Example	
	This example shows how to c	lisable auto-generation ESI type 1:

Router# configure Router(config)# evpn Router(config-evpn)#ethernet-segment Router(config-evpn-es)#type 1 auto-generation-disable

evi

evi

	use the evi		ode and configure optional BGP settings for a bridge domain or EVI, iguration mode. To return to the EVPN configuration mode, use the			
	evi evi-id no evi evi	-id				
Syntax Description	evi-id Spe	ecifies the Ethernet VPN ID t	to set. The range is from 1 to 65534.			
Command Default	None.					
Command Modes	EVPN configuration mode					
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.					
	Use this con	Use this command to configure static BGP route distinguisher or BGP route target for an EVI.				
Task ID	Task Ope ID	•				
	l2vpn rea wri					
	Example					
	This example shows how to enter the EVPN EVI configuration mode:					
	RP/0/RSP0/ RP/0/RSP0/	CPU0:router# configure CPU0:router(config)# ev CPU0:router(config-evpn CPU0:router(config-evpn)# evi 2			
Related Commands	Command		Description			
	evpn, on pa	age 289	Enters EVPN configuration mode.			
	bgp (EVPN), on page 281	Enables BGP in the PBB EVPN configuration.			

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	han Ca	nf anna DCD		
Syntax Description	bgp Co	nfigures BGP.		
	evi Co	nfigures Ethernet VPN ID (H	EVI).	
	interface As	signs an interface to EVPN		
	timers Co	nfigures global EVPN time	TS.	
Command Default	None.			
Command Modes	Global configu	iration		
Command History	Release	Modification		
		This command was introduced.		
Usage Guidelines			er group associated with a task group that includes appropriate task nting you from using a command, contact your AAA administrator	
Task ID	Task Operat ID	ion		
	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)#			
Related Commands	Command		Description	
	evi, on page 2		nters the EVPN EVI configuration mode to configure optional BGP etitings for a bridge domain or EVI.	

Command	Description
interface (EVPN), on page 296	Enters the EVPN Interface configuration mode.
timers, on page 332	Configures timers that affect the convergence of PBB EVPN in failure scenarios.

evpn evi

To enable PBB EVPN and set the EVI for the bridge, use the **evpn** evi command in the L2VPN bridge group bridge domain PBB-core configuration mode. To disable PBB EVPN and reset the EVI, use the **no** form of this command.

evpn evi evi-id **no evpn evi** evi-id

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

Command Default	None.		
Command Modes	L2VPN bri	dge group bridge domain PBB con	e configuration
Command History	Release	Modification	
	Release 4.3.2	This command was introduced.	
Usage Guidelines		iser group assignment is preventin	roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
	The VPN II	D must be unique globally per net	vork.
Taak ID			

 Task ID
 Task ID
 Operation

 ID
 12vpn
 read, write

This example shows how to enable PBB EVPN and set the EVI for the 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 1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# pbb core
```

RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pbb-core) # evpn evi 2 RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pbb-core) #

Related Commands

mands	Command	Description
	evpn, on page 289	Enters EVPN configuration mode.
	l2vpn, on page 69	Enters L2VPN configuration mode.
	pbb, on page 303	Configures the provider backbone bridge core or edge.

flushagain

To configure the MAC flush again timer, use the **flushagain** command in the EVPN Interface Timers configuration or in the EVPN Timers configuration mode. To reset the MAC flushagain timer, use the **no** form of this command.

flushagain seconds no flushagain seconds

<i>seconds</i> Specifies the value in seconds ranging from 0 to 120 seconds. The default value is 60 seconds.		
None.		
EVPN Interface Timers configuration		
EVPN Timers configuration		
Release Modification		
ReleaseThis command was4.3.2introduced.		
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
Task Operation ID		
12vpn read,		
-		

This example shows how to configure the MAC flushagain timer in the EVPN Interface Timers 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)# timers RP/0/RSP0/CPU0:router(config-evpn-ac-timers)# flushagain 20 RP/0/RSP0/CPU0:router(config-evpn-ac-timers)#

This example shows how to configure the MAC flushagain timer in the EVPN Timers configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# timers
RP/0/RSP0/CPU0:router(config-evpn-timers)# flushagain 30
RP/0/RSP0/CPU0:router(config-evpn-timers)#
```

Command	Description
evpn, on page 289	Enters EVPN configuration mode.
interface (EVPN), on page 296	Enters the EVPN Interface configuration mode.
timers, on page 332	Configures timers that affect the convergence of PBB EVPN in failure scenarios.
recovery, on page 307	Configures the recovery timer.
peering, on page 304	Configures the peering timer.
programming, on page 306	Configures the programming timer.
	evpn, on page 289 interface (EVPN), on page 296 timers, on page 332 recovery, on page 307 peering, on page 304

flood-time

To enable flooding of traffic to the entire core bridge when the PBB-VPLS Flood Optimization feature is enabled on the core bridge, use the **flood-time** command in the flood optimization for PBB over VPLS global configuration submode.

	flood-time	seconds	
Syntax Description	seconds Specifies the flood-time in seconds. Range is from 3 to 600 seconds.		
Command Default	Flooding is	disabled during convergence ever	ts.
Command Modes	Flood optimization for PBB over VPLS global configuration submode.		
Command History	Release	Modification	
	Release 5.1.2	This command was introduced.	
Usage Guidelines		iser group assignment is preventin	roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator

Enables flooding of traffic on the entire core bridge when flood-time is enabled on the core bridge. This provides time for MMRP to converge with the affected peer(s) before pruning the traffic. Flooding will be disabled and the core bridge will start pruning the traffic when the flood-time has expired.

Task ID	Task ID	Operation
Iask ID	lask ID	Uperation

ethernet-services read, write

force single-homed

The following example shows how to set the flood-time:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# mmrp-flood-optimization
RP/0/RSP0/CPU0:router(config-mmrp-flood-opt)# flood-time 80
```

force single-homed

To configure force single-homed, use **force single-homed** command in the global configuration mode. To return to the default behavior, use the **no** form of this command.

	no force sin	gle-homed	
Command Default	None		
Command Modes	Global conf	iguration	
Command History	Release	Modification	
	Release 4.3.2	This command was introduced.	
Usage Guidelines		based access redundancy (EVLAG LAG access protection protocol.) designated forwarder elections are disregarded in favor of the
	When CE is directly connected to a PE through a physical or bundle port and the redundant connection another PE is operating an MCLAG redundancy group.		
	Specifically, the ESI assignment to the interface is no longer used for EVPN-based access redun protection mechanisms and the MCLAG redundancy protocol will control the state of this interf		
	With this command only the access protection is relinquished, and EVPN core mechanisms remain operational including any core functionality requiring the use of an ESI. This command is different than assigning ESI-0 to the interface, and functions also with an assigned ESI. With MCLAG control of the interface state, those EVPN core procedures that depend on interface state remain the same.		
	Use this command to force the interface into single homed EVPN mode and interoperate with MCLAG access protection.		
	The following	ng example shows how to configu	re force single-homed.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface GigabitEthernet0/0/0/0
Router(config-evpn-ac)# ethernet-segment force single-homed
```

identifier

To set the Ethernet segment identifier value of an interface, use the **identifier** command in the EVPN interface Ethernet-segment configuration mode. To delete the Ethernet segment identifier value, use the **no** form of this command.

identifier system-priority priority-value system-id system-id no identifier system-priority priority-value system-id system-id

Syntax Description	system-priority Specifies the CE system priority (LACP).			
	<i>priority-value</i> Specifies the LACP system-priority value. The range is from 0 to ffff.			
	system-id	Specifies the CE system ID (LACP).		
	system-id	Specifies the LACP system ID in the H.H.H format.		
Command Default	None.			
Command Modes	EVPN interface I	Ethernet segment configuration mode		
Command History	Release M	odification		
	Release Th 4.3.2	is command was introduced.		
Usage Guidelines		and, you must be in a user group associated with a task group that includes appropriate task roup assignment is preventing you from using a command, contact your AAA administrator		
		d to overwrite computed Ethernet segment identifier value or to set Ethernet segment identifier ace which is not a bundle. The concatenated value is unique per PE.		
Task ID	Task Operatio	n		
	l2vpn read, write	_		
	Example	_		

Example

This example shows how to set the Ethernet segment identifier value of an interface in the EVPN interface Ethernet segment configuration mode:

I

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)# identifier system-priority 2 system-id 1.1	1

Related Commands ^

Command	Description
ethernet-segment, on page 286	Enters EVPN interface ethernet segment configuration mode.
load-balancing-mode, on page 299	Sets the load balancing mode of a physical port or bundle to active-active.
#unique_211	
backbone-source-mac, on page 280	Configures the backbone source MAC address.

join-time (PBB)

To set the join-time for all active ports, use the join-time command in the flood optimization for PBB over VPLS global configuration submode.

join-time milliseconds

Syntax Description	millisecond	-	naximum time for the join timer parameter for all active ports in milliseconds. 100 to 1000 milliseconds.
Command Default	200 millisec	conds	
Command Modes	Flood optim	ization for PBB o	ver VPLS global configuration submode.
Command History	Release	Modification	
	Release 5.1.2	This command	vas introduced.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
	transmitted r	nessages to take in	d to jitter the sending of MMRPDUs on multi-point LANs, allowing any to account received MMRPDUs from multiple peers if they arrive close together. The sender within the range of 0 to join-time.
Task ID	Task ID	Operation	
	ethernet-serv	vices read, write	

The following example shows how to set the join time on all active ports:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# mmrp-flood-optimization
RP/0/RSP0/CPU0:router(config-mmrp-flood-opt)# join-time 300
```

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			es the following interface types connected to device:		
			• Ph	nysical ethernet interface		
			• Bı	• Bundle ethernet		
			For more information about the syntax for the router, use the question mark (?) online help function.			
	interface p	path-id	Physica	al or virtual interface name.		
			The rar	nge 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.		
				re information about the syntax for the router, question mark (?) online help function.		
Command Default	None.					
Command Modes	EVPN con	figuration 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		user group assignment is preventing you		vith a task group that includes appropriate task a command, contact your AAA administrator		

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.

ask 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 289	Enters EVPN configuration mode.	
	ethernet-segment, on page 286	Enters EVPN interface ethernet segment configuration mode.	
	mac-flush mvrp, on page 301	Performs a MAC flush on an Ethernet-segment.	
	timers, on page 332	Configures timers that affect the convergence of PBB EVPN in failure scenarios.	

leaveall-time (PBB)

leaveall-time seconds

To set the leave-all-time for all active ports, use the **leaveall-time** command in the flood optimization for PBB over VPLS global configuration submode.

 Syntax Description
 seconds
 Sets the minimum time in seconds for the leave-all timer parameter for all active ports. Range is from 5 to 30 seconds.

 Command Default
 10 seconds

Command Modes	Flood optimizat	ion for PBB over VPLS	global configuration submode.			
Command History	Release N	Iodification				
	Release T 5.1.2	his command was introc	luced.			
Usage Guidelines			user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator			
		1	now often the leave-all messages are sent. This forces all the peers to laying any registrations or deregistrations that may be lost.			
Task ID	Task ID	Operation				
	ethernet-services	s read, write				
	The following example shows how to set the leave-all time on all active ports:					
	RP/0/RSP0/CPU		rp-flood-optimization -flood-opt)# leaveall-time 20			

leave-time (PBB)

To set the leave-time for all active ports, use the leave-time command in the flood optimization for PBB over VPLS global configuration submode.

	leave-time	seconds		
Syntax Description	seconds S	Sets the leave time for all active po	orts. Range is from 1 to 90 seconds.	
Command Default	30 seconds			
Command Modes	Flood optin	nization for PBB over VPLS globa	l configuration submode.	
Command History	Release	Modification		
	Release 5.1.2	This command was introduced.		
Usage Guidelines		ser group assignment is preventin	roup associated with a task group that in g you from using a command, contact yo	
		6	egistrations stay in the leaving state before tale registrations is performed after unre	U ,

The leaveall-time and the leave-time commands together control the garbage collection.

The IEEE specification states that the value of the **leave-time** command must be less than the value of the **leaveall-time** command.

However, in Cisco IOS-XR, processing outages of several seconds can occur during a process restart or Router Processor Fail-Over (RPFO) leading to a loss of messages.

Therefore, a greater default **leave-time** *value* (thrice that of the **leaveall-time** *value* command) increases the robustness of the Multiple MAC Registration Protocol (MMRP) during packet loss or system outage.

Task ID Task ID Operation

ethernet-services read, write

The following example shows how to set the leave-time on all active ports:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# mmrp-flood-optimization
RP/0/RSP0/CPU0:router(config-mmrp-flood-opt)# leave-time 80
```

load-balancing-mode

To set the load balancing mode of a physical port or bundle to active-active, use the **load-balancing-mode** command in the EVPN Interface Ethernet segment configuration mode. To disable the load balancing mode from active-active, use the **no** form of this command.

load-balancing-mode per-service no load-balancing-mode per-service

Syntax Description	per-service	Specifies the per-service load balancin
Command Default	Active-active	e per-flow
Command Modes	EVPN interfa	ace Ethernet segment configuration mod
Command Modes Command History	EVPN interfa	ace Ethernet segment configuration mod

Usage Guidelines To use this command, you must be in a user group associated with a task 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 this command in a multi-homing configuration to set the redundancy mode to active-active per service.

In this mode, services that are active on one PoA are not active on the other PoA. Services can be represented by an ISID in case of PBB EVPN.

Task ID	Task ID	Operation					
	l2vpn	read, write					
	Exampl	e					
	This example shows how to set the load balancing mode of a physical port or bundle to active-active:						
	RP/0/R	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)# load-balancing-mode per-service						
	RP/0/R	SP0/CPU0:ro	ter(config-evpn-a	c-es)#			
Related Commands	Comm	and		Description			
	ethern	et-segment, o	n page 286	Enters EVPN interface ethernet segment configuration mode.			
	backb	one-source-m	ac, on page 280	Configures the backbone source MAC address.			

mmrp-flood-optimization

To enable flood optimization for PBB over VPLS, use the **mmrp-flood-optimization** command on the core bridge in the PBB core configuration submode. To disable the flood optimization for PBB over VPLS, use the **no** form of this command.

mmrp-flood-optimization no mmrp-flood-optimization

This command has no keywords or arguments.		
Disabled.		
PBB core c	onfiguration	
Release	Modification	
Release 5.1.2	This command was introduced.	
	Disabled. Disabled. PBB core c Release Release	

Usage Guidelines Flood optimization is enabled on all the pseudo-wires in the VFI associated with the core bridge domain. This feature is supported only in the standard full mesh topology of a VPLS network.

Task ID

L

Task
IDOperation12vpnread,
write

mac-flush mvrp

The following example shows how to enable flood optimization for PBB over VPLS:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# bridge group pbb
RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain pbb-core
RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# pbb core
RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-pbb-core)# mmrp-flood-optimization
RP/0/RSP0/CPU0:router(config-12vpn-bg-bd-pbb-core)# end
```

mac-flush mvrp

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.

	no mac-flush mvrp
Syntax Description	mvrp Specifies the MAC flush over MVRP.
Command Default	STP-TCN
Command Modes	EVPN interface configuration
Command History	Release Modification
	ReleaseThis command was4.3.2introduced.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
Task ID	Task Operation ID
	l2vpn read, write
	This example shows how to perform the MAC flush over MVRP on an Ethernet segment:
	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)# mac-flush mvrp RP/0/RSP0/CPU0:router(config-evpn-ac)#				
Related Commands	Command	Description			
	interface (EVPN), on page 296	Enters the EVPN Interface configuration mode.			

mode singleton

To enable singleton ICCP mode, use the **mode** singleton command in the Redundancy ICCP group configuration mode. To disable singleton ICCP mode, use the **no** form of this command.

	mode singleton no mode singleton		
Syntax Description	This command has no arguments or keywords.		
Command Default	None.		
Command Modes	Redundancy ICCP group configuration		
Command History	Release Modification		
	ReleaseThis command was introduced.4.3.2		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
Task ID	Task Operation ID		
	l2vpn read, write		
	This example shows how to enable singleton ICCP mode:		
	RP/0/RSP0/CPU0:router# configure		

```
RP/0/RSP0/CPU0:router(config)# redundancy
RP/0/RSP0/CPU0:router(config-redundancy)# iccp
RP/0/RSP0/CPU0:router(config-redundancy-iccp)# group 1
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mode singleton
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)#
```

pbb

To configure the provider backbone bridge core or edge, use the **pbb** command in the bridge domain configuration submode. To return to the default behavior, use the **no** form of this command.

pbb {edge i-sid service-id core-bridge core-bridge-domain-name | core}
no pbb {edge i-sid service-id core-bridge core-bridge-domain-name | core}

Syntax Description	edge	Configures the PBB edge.		
	i-sid	Specifies the service instance identifier. The ranges is from 256 to 16777214.		
		Note The 16777215 (0xFFFFFF) service instance identifier is reserved for wildcard.		
	service-id	Service instance identifier.		
	core-bridge	Specifies the name of the core-bridge domain connected to that edge-bridge domain.		
	core-bridge-domain-name	Core bridge domain name.		
	core	Configures the PBB core.		
Command Default	None			
Command Modes	L2VPN bridge group bridg	ge domain configuration		
Command History	Release Modificatio	 Dn		
	Release 3.9.1 This community introduced.			
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate ta IDs. If the user group assignment is preventing you from using a command, contact your AAA administra for assistance.			
	This command allows you	to enter pbb edge configuration mode or pbb core configuration mode.		
Task ID	Task Operations ID			
	l2vpn read, write			
Examples	The following example sho	ows how to configure the PBB edge component:		
	config l2vpn			

```
bridge group PBB
bridge-domain PBB-EDGE
interface GigabitEthernet0/0/0/38.100
!
interface GigabitEthernet0/2/0/30.150
!
pbb edge i-sid 1000 core-bridge PBB-CORE
!
!
```

The following example shows how to configure the PBB core component:

```
config
l2vpn
bridge group PBB
bridge-domain PBB-CORE
interface G0/5/0/10.100
!
interface G0/2/0/20.200
!
pbb core
!
!
```

Related Commands	Command	Description
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	Enters L2VPN configuration mode.

peering

To configure the peering timer, use the **peering** command in the EVPN Timers configuration mode. To delete the peering timer, use the **no** form of this command.

	peering seconds no peering seconds		
Syntax Description	<i>seconds</i> Specifies the value in seconds ranging from 0 to 300 seconds. The default value is 45 seconds.		
Command Default	None.		
Command Modes	EVPN Timers 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.

In a single homed Ethernet segment, wait for this timer to expire before advertising BGP route target, Ethernet segment identifier (ESI), and local MAC.

 Task ID
 Task D
 Operation ID

 12vpn
 read, write

This example shows how to configure the peering timer in the EVPN Timers configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# timers
RP/0/RSP0/CPU0:router(config-evpn-timers)# peering 30
RP/0/RSP0/CPU0:router(config-evpn-timers)#
```

Related Commands	Command	Description	
	evpn, on page 289	Enters EVPN configuration mode.	
	timers, on page 332	Configures timers that affect the convergence of PBB EVPN in failure scenarios.	
	flushagain, on page 291	Configures the MAC flushagain timer.	
	recovery, on page 307	Configures the recovery timer.	
	programming, on page 306	Configures the programming timer.	

periodic transmit (PBB)

To enable periodic Multiple MAC Registration Protocol Data Units (MMRPDUs), use the **periodic transmit** command in the flood optimization for PBB over VPLS global configuration submode.

	periodic transmit [into	erval seconds]
Syntax Description	1	cifies the periodic transmit interval in seconds. Range is from 2 to 10. If the interval word is not specified, then the value defaults to 3 seconds.
Command Default	Periodic MMRPDUs are disabled.	
Command Modes	Flood optimization for PBB over VPLS global 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 can optionally be used to configure the protocol to replay data periodically. This is in addition to the periodic replay triggered by the leave-all timer. The use of this command will not be necessary in the vast majority of deployments and enabling it can cause a significant increase in CPU usage.				
Task ID	Task ID	Operation			
	ethernet-ser	vices read, write			
	The following example shows how to enable periodic MMRPDUs transmitted on all active ports:				
	RP/0/RSP0/	RP/0/RSP0/CPU0:router# configure			

RP/0/RSP0/CPU0:router(config)# mmrp-flood-optimization RP/0/RSP0/CPU0:router(config-mmrp-flood-opt)# periodic transmit interval 3

programming

To configure the programming timer, use the **programming** command in the EVPN Timers configuration mode. To delete the programming timer, use the **no** form of this command.

programming microseconds no programming microseconds

		C	
Syntax Description	<i>microseconds</i> Specifies the value in microseconds ranging from 0 to 100000 seconds. The default value is 1500 microseconds.		
Command Default	None.		
Command Modes	EVPN Timers configuration		
Command History	Release	Modification	
	Release 4.3.2	This command was introduced.	
Usage Guidelines		er group assignment is preve	er group associated with a task group that includes appropriate task nting you from using a command, contact your AAA administrator

Every time the ES Manager runs DF election, it starts a programming timer to account for the time needed by the hardware to apply the new carving. At the expiry time, the next ES route object is processed or carved, restarting the timer.

Task ID	Operation	
l2vpn	read, write	

This example shows how to configure the programming timer in the EVPN Timers configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# timers
RP/0/RSP0/CPU0:router(config-evpn-timers)# programming 5000
RP/0/RSP0/CPU0:router(config-evpn-timers)#
```

Related Commands C

Command	Description
evpn, on page 289	Enters EVPN configuration mode.
timers, on page 332	Configures timers that affect the convergence of PBB EVPN in failure scenarios.
flushagain, on page 291	Configures the MAC flushagain timer.
recovery, on page 307	Configures the recovery timer.
peering, on page 304	Configures the peering timer.

recovery

To configure the recovery timer, use the **recovery** command in the EVPN Interface Timers configuration or in the EVPN Timers configuration mode. To delete the recovery timer, use the **no** form of this command.

	recovery seconds no recovery seconds
Syntax Description	<i>seconds</i> Specifies the value in seconds ranging from 20 to 3600 seconds. The default value is 20 seconds.
Command Default	None.
Command Modes	EVPN Interface Timers configuration
	EVPN Timers configuration

Command History	Release	Modification		
	Release 4.3.2	This command was introduced.		
Usage Guidelines		user group assignment is pre-	user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator	
			sing the port state UP event in order to give the CE running STP to onditions are already met, this timer is skipped to not add any more	
Task ID	Task Ope ID	eration		
	l2vpn rea wr			
	This examp mode:	le shows how to configure th	e recovery timer in the EVPN Interface Timers configuration	
	<pre>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)# timers RP/0/RSP0/CPU0:router(config-evpn-ac-timers)# recovery 50 RP/0/RSP0/CPU0:router(config-evpn-ac-timers)# This example shows how to configure the recovery timer in the EVPN Timers configuration mode:</pre>			
	RP/0/RSP0, RP/0/RSP0, RP/0/RSP0,	/CPU0:router# configure /CPU0:router(config)# ev /CPU0:router(config-evpn /CPU0:router(config-evpn /CPU0:router(config-evpn)# timers -timers)# recovery 300	
Related Commands	Command		Description	
	evpn, on p	age 289	Enters EVPN configuration mode.	
	interface (interface (EVPN), on page 296 Enters the EVPN Interface configuration mode.		
	timers, on	timers, on page 332 Configures timers that affect the convergence of PBB failure scenarios.		
	flushagain	, on page 291	Configures the MAC flushagain timer.	
	peering, or	1 page 304	Configures the peering timer.	
		ing, on page 306	Configures the programming timer.	

rewrite ingress tag push

To configure the backbone VLAN ID for a PBB core bridge, use the **rewrite ingress tag push** command in the PBB core configuration mode. To return to the default behavior, use the **no** form of this command.

	rewrite ingress tag push dot1ad vlan-id symmetric
Syntax Description	dot1ad Indicates that the IEEE 802.1ad provider bridges encapsulation type is used.
	<i>vlan-id</i> VLAN ID. Range is from 1 to 4094.
	symmetric Specifies that all rewrites must be symmetric.
Command Default	None
Command Modes	PBB core configuration
Command History	Release Modification
	Release 3.9.1 This command was introduced.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
Task ID	Task Operations ID
	l2vpn read, write
Examples	The following example shows how to configure the backbone VLAN ID for the PBB core bridge:
	<pre>config l2vpn bridge group PBB bridge-domain PBB-CORE interface G0/5/0/10.100 ! interface G0/2/0/20.200 ! pbb core rewrite ingress tag push dotlad 100 symmetric !</pre>

I

! !

Related Commands	Command	Description
	bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
	bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
	l2vpn, on page 69	Enters L2VPN configuration mode.
	pbb, on page 303	Configures the provider backbone bridge core or edge.

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	e-df-weight }]

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.	
Command Default	Automatic service ca	arving	
Command Modes	EVPN interface Ethe	ernet segment configuration mode	
Command History	Release Modif	fication	
	Release This c 6.1.2	command was introduced.	

Release	Modification
Release	The follwing keywords are added:
7.3.1	 preference-based
	 access-driven

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
```

Example

This example shows how to sepcify 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 01.11.00.00.00.00.00.00.00.00
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)#access-driven
Router(config-evpn-ac-es-sc-pref)#commit
```

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.

I

	esi	Filters by Etherne	et Segment ider	tifier.	
	interface Filters by interface name.				
	location	Displays location	specific inform	nation.	
	private	Displays private	information.		
	standby	Displays standby	node specific ir	formation.	
Command Default	None.				
Command Modes	EXEC				
Command History	Release	Modification		_	
	Release 4.3.2	This command	l was introduced	-	
Usage Guidelines	s To use this command, you must be in a user group associated with a task group that includes appropriat IDs. If the user group assignment is preventing you from using a command, contact your AAA administ for assistance.				
Task ID	Task Op ID	peration			
	l2vpn rea	ad			
	Example				
	This sample output shows the EVPN Ethernet segment with interface filter:				
	Ethernet S	Segment Id	Interface	net-segment interface gigabitethernet 0/3/0/0 detail Nexthops	
		.9e00.0210.0000		1.100.100.100	
	be01.0300.	.be01.ce00.0001	BE1	2.100.100.100 1.100.100.100 2.100.100.100	
	be02.0300.	.be02.0101.0002	BE2	2.100.100.100 1.100.100.100 2.100.100.100	
	N/A		Gi0/3/0/3	N/A	
	This sample	e output shows the	e EVPN Ethern	et segment detailed information:	
	RP/0/RSP0/CPU0:router# show evpn ethernet-segment detail Tue Jun 25 14:17:09.610 EDT Legend:				
		EVPN load-balan ridge Ports PBB	-	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 : Up State 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 : 0 Elected 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 : Up State Redundancy : Active urce MAC : 0024.be01.ce00 (Local) Source MAC 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 289	Enters EVPN configuration mode.
	ethernet-segment, on page 286	Enters EVPN interface ethernet segment configuration mode.

show evpn evi

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

	<pre>show evpn evi ac- }]</pre>	<i>id</i> [{bridge-domain detail inclusive-multicast location mac standby v]	pn-id
Syntax Description	ac-id	Specifies the attachment circuit id.	
	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 Modif	cation	
	Release This c 4.3.2	ommand was introduced.	_
	Release The va 6.0.0	riable <i>ac-id</i> was added	
	Release The sh 6.1.2	ow command output is enhanced to display the Service Path Preference parameter	<u>s</u> .
Usage Guidelines		this module, you must be in a user group associated with a task group that include If the user group assignment is preventing you from using any command, contact or assistance.	

Task ID

Task
IDOperation12vpnread

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	1.be03.ce0	01
MAC address	Nexthop	Label	vpn-id
0024.be03.ce01	3.100.100.100	16004	185
	4.100.100.100	16004	185
ESI port ke	y : 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:

<pre>RP/0/RSP0/CPU0:router#show e ISID: 1850312, Originating I Nexthop: :: Label : 16005</pre>	evpn evi inclusive-multicast detail IP: 1.100.100.100	185
Source : Local ISID: 1850312, Originating I Nexthop: 2.100.100.100 Label : 16005	P: 2.100.100.100	185
Source : Remote ISID: 1850312, Originating I Nexthop: 3.100.100.100 Label : 16005	EP: 3.100.100.100	185
Source : Remote ISID: 1850312, Originating I Nexthop: 4.100.100.100 Label : 16005 Source : Remote	EP: 4.100.100.100	185

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

RP/0/RSP0/	CPU0:router#show evpr	n evi bridge-domain	tb1-core1 d	detail
EVI	Bridge Domain	Туре		
145	tbl-corel	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 PBB 165 tb1-core2 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 Туре _____ 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 Tvpe ----- -----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 Tvpe ----- -----0100.9e00.0210 Import 0100.be01.ce00 Import 0100.be02.0101 Import

This example displays the detailed information about **show evpn evi** command. The output provides an overview of the state of the globally configured features.

RP/0/RSP0/CPU0:router# show evpn evi ac-id detail Mon Apr 18 13:16:46.597 EDT VPN ID Source AC ID Target AC ID

110	10	30
200	1	3
200	4	6
200	11	13

This sample output shows the EVPN EVI detailed information with service path preference parameters:

RP/0/RSP0/CPU0:router#show evpn evi vpn-id 1 detail Mon Jun 20 21:28:42.413 EDT EVI Bridge Domain Type 1 core1 PBB Unicast Label : 24000 Multicast Label: 24001 Flow Label: N Control-Word: Enabled Table-policy Name: fwd2 Forward-class: 2 RD Config: none RD Auto : none RT Auto : none Route Targets in Use Туре _____ ____

Related Commands	Command	Description
	evpn, on page 289	Enters EVPN configuration mode.
	evi, on page 288	Enters the EVPN EVI configuration mode to configure optional BGP settings for a bridge domain or EVI.

show evpn summary

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

	show evp	on 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
                          : f866.f214.abd7
PBB BSA MAC address
FBB BSA MAC address: 1866.f214.abd7Global peering timer: 45 secondsGlobal 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 Comman

Command

evpn, on page 289

Enters EVPN configuration mode.

show I2vpn bridge-domain pbb

To display the provider backbone bridge details, use the **show l2vpn bridge-domain pbb** command in EXEC mode.

Description

show l2vpn bridge-domain pbb {core [{brief|detail|hardware|private}]|edge [{brief|core-bridge
| detail|hardware|private}]|i-sid service-id [{brief|detail|hardware|private}]}

detail Displays detailed information about the PBB core, edge or service instance id hardware Displays hardware information. private Displays private information about the PBB core, edge or service instance id core-bridge Displays the name of the core-bridge domain connected to the edge-bridge d Command Default None Command Modes I2vpn Command History Release Release 3.9.1 This command was introduced. To use this command, you must be in a user group associated with a task group that includes IDs. If the user group assignment is preventing you from using a command, contact your Aafor assistance. Task ID Task Operations I2vpn read	yntax Description		
Isid Displays the service instance identifier. service-id Service ID. brief Displays brief information about the PBB core, edge or service instance identifier. detail Displays detailed information about the PBB core, edge or service instance identifier. privat Displays detailed information about the PBB core, edge or service instance identifier. privat Displays hardware information. private Displays private information about the PBB core, edge or service instance identifier. core-bridge Displays the name of the core-bridge domain connected to the edge-bridge domain connected to the edge-bridge domain connected to the edge-bridge domain about the PBB core, edge or service instance. Command Default None Command Modes I2vpn Command History Release Release is 3.9.1 This command was introduced. To use this command, you must be in a user group associated with a task group that includee IDs. If the user group assignment is preventing you from using a command, contact your Ac for assistance. Task ID Task Operations ID I2vpn read Examples The following examples shows the output from the show I2vpn bridge-domain pbb command splay private information is 1234 Pridge group: g2, bridge-domain isid 1234 Bridge g		core	Displays the PBB core.
service-id Service ID. brief Displays brief information about the PBB core, edge or service instance iden detail Displays detailed information about the PBB core, edge or service instance iden detail Displays detailed information about the PBB core, edge or service instance iden detail Displays detailed information about the PBB core, edge or service instance iden private Displays private information about the PBB core, edge or service instance iden core-bridge Displays the name of the core-bridge domain connected to the edge-bridge domain Command Default None Command Modes I2vpn Command History Release Release Modification Release Modification Release In use this command, you must be in a user group associated with a task group that includee IDs. If the user group assignment is preventing you from using a command, contact your Aufor assistance. Task Operations ID I2vpn id 12vpn tridge droup: q2, bridge-domain isid 1234 pridge group: q2, bridge-domain: pb		edge	Displays the PBB edge.
brief Displays brief information about the PBB core, edge or service instance iden detail Displays detailed information about the PBB core, edge or service instance iden detail Displays hardware information. private Displays private information about the PBB core, edge or service instance id core-bridge Displays private information about the PBB core, edge or service instance id core-bridge Displays the name of the core-bridge domain connected to the edge-bridge d Command Default None Command Modes 12vpn Command History Release Modification Release Modification Release Modification Release In use this command, you must be in a user group associated with a task group that includee Ds. If the user group assignment is preventing you from using a command, contact your Aufor assistance. Task Operations 12vpn read tstow 12vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, shgId: 0, MSTi: Type: pbb-edge, 1-2121 Aging: 300 s, M&C IImit: 4000, Action: none, Notification: syslog PBE Edge, state: up, Static MAC addresses: 0 List of PBB: PBE Edge, state:		i-sid	Displays the service instance identifier.
detail Displays detailed information about the PBB core, edge or service instance id hardware Displays hardware information. private Displays private information about the PBB core, edge or service instance id core-bridge Displays private information about the PBB core, edge or service instance id core-bridge Displays the name of the core-bridge domain connected to the edge-bridge d Command Default None Command Modes 12vpn Command History Release Release Modification Release 3.9.1 This command was introduced. Jsage Guidelines To use this command, you must be in a user group associated with a task group that includes IDS. If the user group assignment is preventing you from using a command, contact your Ac for assistance. Fask ID Task Operations ID 12vpn read Examples The following examples shows the output from the show 12vpn bridge-domain pbb command show 12vpn bridge-domain isid 1234 Bridge group: q2, bridge-domain isid 1234 Bridge group: q2, bridge-domain: bbb-bd1, id: 1, state: up, Shgld: 0, MST1: Type: pbb-edge, T-SID: 1224 Aging: 300 s, MC Linut: 4000, Action: none, Notification: syslog Pilter MAC addresses: 0 Acs: 1 (1 up), VTIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of Acs: </td <td></td> <td>service-id</td> <td>Service ID.</td>		service-id	Service ID.
hardware Displays hardware information. private Displays private information about the PBB core, edge or service instance id core-bridge command Default None Command Modes 12vpn Command Mistory Release 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 IDs. If the user group assignment is preventing you from using a command, contact your A. for assistance. Fask ID Task Operations I 12vpn Preventing you from using a command, contact your A. for assistance. Examples The following examples shows the output from the show 12vpn bridge-domain pbb command, sontact your A. for assistance. Examples The following examples shows the output from the show 12vpn bridge-domain pbb command, sontact your A. for assistance. Examples The following examples shows the output from the show 12vpn bridge-domain pbb command, sontact your A. for assistance. Examples The following examples shows the output from the show 12vpn bridge-domain pbb command, sontact your A. for assistance. Examples The following examples shows the output from the show 12vpn bridge-domain pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: Type: pb=edge, T-STD: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog riller		brief	Displays brief information about the PBB core, edge or service instance identifier.
private Displays private information about the PBB core, edge or service instance id core-bridge Displays the name of the core-bridge domain connected to the edge-bridge d Command Default None I2vpn I2vpn Command History Release Release 3.9.1 This command was introduced. Jsage Guidelines To use this command, you must be in a user group associated with a task group that includes IDs. If the user group assignment is preventing you from using a command, contact your Ax for assistance. Task D I2vpn I2vpn Examples The following examples shows the output from the show I2vpn bridge-domain pbb command. So, MAC limit: 4000, Action: none, Notification: syslog #show 12vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 Acts: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBs: 1 (1 up) List of PEBs: PB Edge, state: up, Static MAC addresses: 0 List of Acts: Gl0/2/0/0, state: up, Static MAC addresses: 2, MSTI: 0		detail	Displays detailed information about the PBB core, edge or service instance identifier
core-bridge Displays the name of the core-bridge domain connected to the edge-bridge d Command Default None Command Modes I2vpn Command History Release Release Modification Release 3.9.1 This command was introduced. Isage Guidelines To use this command, you must be in a user group associated with a task group that includes IDs. If the user group assignment is preventing you from using a command, contact your A. for assistance. Task D Task Operations ID I2vpn read Examples The following examples shows the output from the show I2vpn bridge-domain pbb comm #show 12vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, T-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Pilter MAC addresses: 0 NAC addresses: 0 NAC addresses: 0 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0		hardware	Displays hardware information.
Command Default None Command Modes I2vpn Command History Release Modification Release 3.9.1 This command was introduced. Jsage Guidelines To use this command, you must be in a user group associated with a task group that includes IDs. If the user group assignment is preventing you from using a command, contact your A. for assistance. Fask ID Task Operations ID I2vpn read I2vpn read Examples The following examples shows the output from the show I2vpn bridge-domain pbb comm #show 12vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 AC: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PB Edge, state: up, Static MAC addresses: 0 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0		private	Displays private information about the PBB core, edge or service instance identifier
Command Modes I2vpn Command History Release Modification Release 3.9.1 This command was introduced. Jsage Guidelines To use this command, you must be in a user group associated with a task group that includes IDs. If the user group assignment is preventing you from using a command, contact your Au for assistance. Fask ID Task Operations ID I2vpn read I2vpn read Examples The following examples shows the output from the show I2vpn bridge-domain pbb command string group: g2, bridge-domain: jbb-bdl, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, T-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIS: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state: up, Static MAC addresses: 0 List of PBBs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0		core-bridge	Displays the name of the core-bridge domain connected to the edge-bridge domain.
Command Modes 12vpn Release Modification Release 3.9.1 This command was introduced. Jsage Guidelines To use this command, you must be in a user group associated with a task group that includes IDs. If the user group assignment is preventing you from using a command, contact your As for assistance. Fask ID Task Operations ID ID 12vpn read Examples The following examples shows the output from the show I2vpn bridge-domain pbb comm #show 12vpn bridge-domain isid 1234 Bridge group: 92, bridge-domain ipbb-bdl, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIS: 0, PMS: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state: up, Static MAC addresses: 0 List of ACS: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0	ommand Default	None	
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 IDs. If the user group assignment is preventing you from using a command, contact your A. for assistance. Task ID Task Operations ID I2vpn read Examples The following examples shows the output from the show 12vpn bridge-domain pbb comm #show 12vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 Acs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0		l2vpn	
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 IDs. If the user group assignment is preventing you from using a command, contact your A. for assistance. Task ID Task Operations ID I2vpn read I2vpn read Examples The following examples shows the output from the show I2vpn bridge-domain pbb comm #show 12vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBE Rdge, state: up, Static MAC addresses: 0 List of ACS: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0			
Jsage Guidelines To use this command, you must be in a user group associated with a task group that includes IDs. If the user group assignment is preventing you from using a command, contact your A. for assistance. Fask ID Task Operations ID I2vpn read I2vpn read Examples The following examples shows the output from the show I2vpn bridge-domain pbb commets for a sistence, ISB Pridge group: g2, bridge-domain: pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0	ommand History	Release	Modification
ID I2vpn read Examples The following examples shows the output from the show l2vpn bridge-domain pbb comm #show l2vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state: up, Static MAC addresses: 0 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0	sage Guidelines	IDs. If the us	er group assignment is preventing you from using a command, contact your AAA adr
Examples The following examples shows the output from the show l2vpn bridge-domain pbb comm #show l2vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state: up, Static MAC addresses: 0 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0	ask ID	•	rations
<pre>#show l2vpn bridge-domain isid 1234 Bridge group: g2, bridge-domain: pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state: up, Static MAC addresses: 0 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0</pre>			
<pre>Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state: up, Static MAC addresses: 0 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0</pre>		l2vpn read	
For IOS-XR 5.3.1 and earlier releases.	xamples		
	xamples	The followin #show 12vpn Bridge grou Type: pb Aging: 30 Filter MA ACs: 1 (1 u List of PBB PBB Edg List of	g examples shows the output from the show l2vpn bridge-domain pbb command: h bridge-domain isid 1234 up: g2, bridge-domain: pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: 0 bb-edge, I-SID: 1234 00 s, MAC limit: 4000, Action: none, Notification: syslog AC addresses: 0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) 3s: ge, state: up, Static MAC addresses: 0 : ACs:
#show l2vpn bridge-domain detail isid 1234 Bridge group: g2, bridge-domain: pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: Type: pbb-edge, I-SID: 1234	xamples	The followin #show l2vpn Bridge grou Type: pb Aging: 30 Filter MA ACs: 1 (1 u List of PBB PBB Edg List of Gi0/2/0	g examples shows the output from the show l2vpn bridge-domain pbb command: a bridge-domain isid 1234 ap: g2, bridge-domain: pbb-bdl, id: 1, state: up, ShgId: 0, MSTi: 0 bb-edge, I-SID: 1234 00 s, MAC limit: 4000, Action: none, Notification: syslog AC addresses: 0 ap), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) Bs: ge, state: up, Static MAC addresses: 0 ACs: 0/0, state: up, Static MAC addresses: 2, MSTi: 0

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 _____ I 222.333.444 777.888.999 333.444.555 888.999.111 Statistics: packet totals: receive 3919680, send 9328 byte totals: receive 305735040, send 15022146 List of ACs: AC: GigabitEthernet0/1/0/0, state is up Type Ethernet MTU 1500; XC ID 0x2000001; interworking none; MSTi 0 MAC learning: enabled Flooding: Broadcast & Multicast: enabled Unknown unicast: enabled MAC aging time: 300 s, Type: inactivity MAC limit: 4000, Action: none, Notification: syslog MAC limit reached: yes Security: disabled DHCPv4 snooping: disabled Static MAC addresses: 0000.0000.0000 0001.0002.0003 Statistics: packet totals: receive 3919680, send 9328 byte totals: receive 305735040, send 15022146

For IOS-XR 5.3.2 release.

```
#show l2vpn bridge-domain detail isid 1234
Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
Type: pbb-edge, I-SID: 1234
Core-bridge: pbb-bd2
```

MAC learning: enabled

MAC withdraw: disabled Flooding: Broadcast & Multicast: enabled Unknown unicast: enabled MAC aging time: 300 s, Type: inactivity MAC limit: 4000, Action: none, Notification: syslog MAC limit reached: yes Security: disabled DHCPv4 snooping: disabled MTU: 1500 Filter MAC addresses: ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state is up XC ID 0x2000001 MAC learning: enabled Flooding: Broadcast & Multicast: enabled Unknown unicast: enabled MAC aging time: 300 s, Type: inactivity MAC limit: 4000, Action: none, Notification: syslog MAC limit reached: yes Split Horizon Group: none DHCPv4 snooping: disabled IGMP Snooping profile: Storm Control: disabled Unknown-unicast-bmac: 666.777.888 CMAC to BMAC Mapping Table: CMAC | BMAC _____ _____ 222.333.444 | 777.888.999 333.444.555 | 888.999.111 Statistics: packets: received 1000 (unicast 1000), sent 0 bytes: received 128000 (unicast 128000), sent 0 MAC move: 10 List of ACs: AC: GigabitEthernet0/1/0/0, state is up Type Ethernet MTU 1500; XC ID 0x2000001; interworking none; MSTi 0 MAC learning: enabled Flooding: Broadcast & Multicast: enabled Unknown unicast: enabled MAC aging time: 300 s, Type: inactivity MAC limit: 4000, Action: none, Notification: syslog MAC limit reached: yes Security: disabled DHCPv4 snooping: disabled Static MAC addresses: 0000.0000.0000 0001.0002.0003 Statistics: packets: received 3919680, (multicast 0, broadcast 0, unknown unicast 0, unicast 3919680.), sent 9328 bytes: received 305735040 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent 15022146 MAC move: 0

#show 12vpn bridge-domain pbb edge

Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShqId: 0, MSTi: 0 Type: pbb-edge, I-SID: 1234 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state: up, Static MAC addresses: 2 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0 Bridge group: g2, bridge-domain: pbb-bd3, id: 3, state: up, ShgId: 0, MSTi: 0 Type: pbb-edge, I-SID: 2345 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: EDGE, state: up, Static MAC addresses: 2 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0 Bridge group: g2, bridge-domain: pbb-bd4, id: 4, state: up, ShgId: 0, MSTi: 0 Type: pbb-edge, I-SID: 3456 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog Filter MAC addresses: 0 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up) List of PBBs: PBB Edge, state: up, Static MAC addresses: 2 List of ACs: Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0

For IOS-XR 5.3.2 release.

```
#show 12vpn bridge-domain pbb-edge detail
Bridge group: g2, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
 Type: pbb-edge, I-SID: 1234
  Core-bridge: pbb-bd2
 MAC learning: enabled
 MAC withdraw: disabled
  Flooding:
   Broadcast & Multicast: enabled
   Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: yes
  Security: disabled
  DHCPv4 snooping: disabled
  MTU: 1500
  Filter MAC addresses:
  ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up
  List of PBBs:
    PBB Edge, state is up
      XC ID 0x2000001
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
       Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: yes
      Split Horizon Group: none
      DHCPv4 snooping: disabled
      IGMP Snooping profile:
      Storm Control: disabled
```

```
Unknown-unicast-bmac: 666.777.888
     CMAC to BMAC Mapping Table:
        CMAC | BMAC
        _____
                     | 777.888.999
        222.333.444
        333.444.555
                            888.999.111
                       Statistics:
       packets: received 1000 (unicast 1000), sent 0
       bytes: received 128000 (unicast 128000), sent 0
       MAC move: 10
  List of ACs:
   AC: GigabitEthernet0/1/0/0, state is up
     Type Ethernet
     MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
     MAC learning: enabled
     Flooding:
       Broadcast & Multicast: enabled
       Unknown unicast: enabled
     MAC aging time: 300 s, Type: inactivity
     MAC limit: 4000, Action: none, Notification: syslog
     MAC limit reached: yes
     Security: disabled
     DHCPv4 snooping: disabled
     Static MAC addresses:
       0000.0000.0000
       0001.0002.0003
     Statistics:
       packets: received 1000 (unicast 1000), sent 0
       bytes: received 128000 (unicast 128000), sent 0
       MAC move: 10
#show 12vpn bridge-domain pbb-core
Bridge group: g2, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
 Type: pbb-core
 Number of associated pbb-edge BDs: 1
 Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
 Filter MAC addresses: 0
 ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up
 List of PBBs:
   PBB Core, state: up
 List of ACs:
   Gi0/2/0/0, state: up, Static MAC addresses: 2, MSTi: 0
#show 12vpn bridge-domain pbb-core detail
Bridge group: g2, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
 Type: pbb-core
 Number of associated pbb-edge BDs: 1
 MAC learning: enabled
 MAC withdraw: disabled
 Flooding:
   Broadcast & Multicast: enabled
   Unknown unicast: enabled
 MAC aging time: 300 s, Type: inactivity
 MAC limit: 4000, Action: none, Notification: syslog
 MAC limit reached: yes
  Security: disabled
 DHCPv4 snooping: disabled
 MTU: 1500
 Filter MAC addresses:
ACs: 1 (1 up), PBB: 1
List of PBBs:
```

```
PBB Core, state is up
     Vlan-id: 1; XC ID 0x2000001
     MAC learning: enabled
     Flooding:
       Broadcast & Multicast: enabled
       Unknown unicast: enabled
     MAC aging time: 300 s, Type: inactivity
     MAC limit: 600, Action: none, Notification: syslog
     MAC limit reached: no
     Security: disabled
     Split Horizon Group: none
     DHCPv4 snooping: profile foo
     IGMP Snooping profile:
     Storm Control: disabled
  List of ACs:
   AC: GigabitEthernet0/1/0/0, state is up
     Type Ethernet
     MTU 1500; XC ID 0x2000001; interworking none; MSTi 0
     MAC learning: enabled
     Flooding:
       Broadcast & Multicast: enabled
       Unknown unicast: enabled
     MAC aging time: 300 s, Type: inactivity
     MAC limit: 4000, Action: none, Notification: syslog
     MAC limit reached: yes
     Security: disabled
     DHCPv4 snooping: disabled
     Static MAC addresses:
       0000.0000.0000
       0001.0002.0003
     Statistics:
       packet totals: receive 3919680, send 9328
       byte totals: receive 305735040, send 15022146
#show l2vpn bridge-domain pbb-edge core-bridge core-bd brief
Bridge Group/?????????????????? ID State Num ACs/up
                                                              Num PWs/up
Bridge-Domain Name
_____
                   _____ ____
bg/pbb-bdl ??????????????? up
                                                    0/0 >>>>>>>>>>>>>>>
                                      up
0/0 ????????0/0
up
                                                    0/0 ????????0/0
RP/0/0/CPU0:ios#show l2vpn bridge-domain pbb edge core-bridge bd
Bridge group: bg, bridge-domain: pbb-bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Type: pbb-edge, I-SID: 4001
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
 Filter MAC addresses: 0
  ACs: 0 (0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
  List of PBBs:
   PBB Edge, state: up, Static MAC addresses: 2
Bridge group: bg, bridge-domain: pbb-bd2, id: 2, state: up, ShgId: 0, MSTi: 0
  Type: pbb-edge, I-SID: 4002
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 0 (0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 1 (1 up)
  List of PBBs:
   PBB Edge, state: up, Static MAC addresses: 1
Bridge group: bg, bridge-domain: pbb-bd3, id: 3, state: up, ShgId: 0, MSTi: 0
  Type: pbb-edge, I-SID: 4003
```

I

sses: 0
PBBs: 1 (1 up)
none, Notification: syslog

Related Commands	Command	Description
	pbb, on page 303	Configures the provider backbone bridge core or edge.

show l2vpn forwarding bridge pbb

To display the PBB bridge forwarding information, use the **show l2vpn forwarding bridge pbb** command in EXEC mode.

show l2vpn forwarding bridge pbb core [{debug|detail|hardware|location|private}]|edge
[{core-bridge|debug|detail|hardware|location|private}]|i-sid service-id [{debug|detail|hardware
|location|private}]

Syntax Description	debug	Displays the debug information	n.
	core	Displays the PBB core.	
	edge	Displays the PBB edge.	
	i-sid service-id	Displays the service instance i	dentifier.
	brief	Displays brief information abo	out the PBB core, edge or service instance identifier.
	detail	Displays detailed information	about the PBB core, edge or service instance identifier.
	hardware	Displays hardware information	n.
	private	Displays private information a	bout the PBB core, edge or service instance identifier.
	core-bridge	Displays the name of the core	-bridge domain connected to the edge-bridge domain.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 3.9.1	This command was introduced.	

To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. Task ID Task Operations ID l2vpn read **Examples** The following example shows the output from the show l2vpn forwarding pbb backbone-source-mac command: #show l2vpn forwarding backbone-source-mac location 0/1/CPU0 333.444.555 The following example shows the output from the show l2vpn forwarding bridge-domain pbb edge location command: RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain pbb edge location 0/1/CPU0 Bridge MAC ID Ports addr Flooding Learning State Bridge-Domain Name 1 1 0 Enabled UP bg1:bd2 1 0 Enabled Enabled UP bg1:bd4 3 bg1:bd5 4 1 0 Enabled Enabled UP The following example shows the output from the show l2vpn forwarding bridge-domain pbb edge core-bridge bg1:bd3 location command: RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain pbb edge core-bridge bg1:bd3 location 0/1/CPU0 Bridge MAC ID Ports addr Flooding Learning State Bridge-Domain Name ----------- ----- ------ ------1 1 0 Enabled UP ba1:bd2 bg1:bd4 3 1 0 Enabled Enabled UP 1 0 Enabled Enabled UP bg1:bd5 4 The following example shows the output from the show l2vpn forwarding bridge-domain pbb core location command: RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain pbb core location 0/1/CPU0 Bridge MAC Bridge-Domain Name ID Ports addr Flooding Learning State -- ----- ------ -------_____ 1 1 0 Enabled Enabled UP bg1:bd3 The following example shows the output from the **show l2vpn forwarding bridge-domain pbb** i-sid 1000 location command: RP/0/RSP0/CPU0:router# show 12vpn forwarding bridge-domain pbb i-sid 1000 location 0/0/CPU0 Thu Aug 13 12:08:16.492 EDT Bridge MAC Bridge-Domain Name ID Ports addr Flooding Learning State _____ ____ PBB: PBB-EDGE 4 2 Enabled Enabled UP 1 **Related Commands** Command Description

I

Command	Description
pbb, on page 303	Configures the provider backbone bridge core or edge.

show l2vpn forwarding pbb backbone-source-mac

To display the provider backbone source MAC forwarding information, use the **show l2vpn forwarding pbb backbone-source-mac** command in EXEC mode.

show l2vpn forwarding pbb backbone-source-mac {debug [{detail | location | private}]] detail [{debug | location node-id}] | location node-id | private}

Syntax Description	debug	Displa	ys the debug information.		-
	detail	Displa	ys the detailed PBB forward	ling information.	-
	location	Specif	ies the location.		-
	node-id	Node	ID.		-
	private	Displa	ys private information.		-
Command Default	None				
Command Modes	EXEC				
Command History	Release	N	lodification		
	Release 3		his command was atroduced.		
Usage Guidelines		e user g			d with a task group that includes appropriate task ng a command, contact your AAA administrator
Task ID	Task O ID)peration	S		
	l2vpn re	ead	_		
Examples			ample shows the output free e-mac command:	om the show l2v J	pn forwarding pbb
	#show 12 333.444.		rwarding backbone-sour	ce-mac locatio	n 0/1/CPU0
Related Commands	Comman	d	[Description	

Command	Description
pbb, on page 303	Configures the provider backbone bridge core or edge.

show I2vpn pbb backbone-source-mac

show l2vpn pbb backbone-source-mac

To display the provider backbone source MAC information, use the **show l2vpn pbb backbone-source-mac** command in EXEC mode.

	snow 12vpn	pbb backbone-source-mac	
Syntax Description	This comman	d has no keywords or argumer	nts.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 3.9.1	This command was introduced.	
Usage Guidelines		r group assignment is prevent	group associated with a task group that includes appropriate task ing you from using a command, contact your AAA administrator
Task ID	Task Opera ID	ions	
	l2vpn read		
Examples	The following	example shows the output from	n the show l2vpn pbb backbone-source-mac command:
	#show l2vpn 0111.0222.03	pbb backbone-source-mac	
Related Commands	Command	[Description
	pbb, on page	303 C	configures the provider backbone bridge core or edge.

show mmrp-flood-optimization

To display the MMRP flood optimization information, use the **show mmrp-flood-optimization** command in the EXEC mode.

Syntax Description	summary		Displays the summary of the current timer values, total number of core bridges, pseudowires, I-SIDs configured, declarations, and registrations.
	mad		Displays the current state of the MRP Attribute Declaration (MAD) component on a pseudowire, for each active attribute value (that is, group B-MAC).
	pw		Indicates the pseudowire.
	neighbor		Indicates the IP address of the neighbor.
	pw-id		Indicates the pseudowire ID.
	statistics		Displays the packet statistics per pseudowire.
	registratio	ns	Displays the I-SIDs that are declared and a list of peers that have made registrations for those I-SIDs
	received		Displays all the I-SIDs where registrations have been received, even if those I-SIDs are not configured locally.
	core-bridg	je	Displays the information about a specific core-bridge.
	bridge-don	nain-name	Core bridge domain name.
	group-nam	e e	Group name.
	isid		Displays information of a specific service instance identifier.
	isid		Service instance identifier.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 5.1.2	This command was introduced.	
Usage Guidelines		iser group assignment is preventing you	associated with a task group that includes appropriate task from using a command, contact your AAA administrator

show mmrp-flood-optimization [{**summary** | **mad** [**pw** *neighbor pw-id*] | **statistics** [**pw** *neighbor pw-id*] | **registrations** [**received**] [**core-bridge** *bridge-domain-name* : *group-name*] [**isid** *isid*]}]

Task ID Task ID Operation

ethernet-services read, write

The following example shows the output from the **show mmrp-flood-optimization summary** command.

```
RP/0/RSP0/CPU0:router#show mmrp-flood-optimization summary
Core Bridges:
                      4
Pseudowires:
                       100
I-SIDs configured:
                     2000
Total MMRP declarations: 200000
Registrations received: 220000
Flood Time:
                disabled
Leaveall Time: 10000 ms
Leave Time:
                30000 ms
Join Time:
                200 ms
Transmit Period: 1000 ms
```

The following example shows the output from the show mmrp-flood-optimization mad command.

```
RP/0/RSP0/CPU0:router#show mmrp-flood-optimization mad
Core-Bridge: PBB-VPLS-Corel PW: neighbor 1.2.3.4, pwid 87
Participant Type: Full; Point-to-Point: Yes
Admin Control: Applicant Normal; Registrar Normal
LeaveAll Passive (next in 5.92s); periodic disabled
Leave in 25.70s; Join not running
Last peer 0293.6926.9585; failed registrations: 0
I-SID B-MAC Applicant Registrar
1 001E.8300.0001 Very Anxious Observer Leaving
16777216 001E.83FF.FFFF Quiet Passive Empty
```

static-mac-address

To map a customer destination MAC address to backbone destination MAC address, use the **static-mac-address** command in the PBB edge configuration mode. To return to the default behavior, use the **no** form of this command.

static-mac-address cust-mac-address bmac bmac-mac-address no static-mac-address cust-mac-address bmac bmac-mac-address

Syntax Description	cust-mac-address	Customer destination MAC address in hexadecimal format.
	bmac	Specifies that the static backbone MAC address must be mapped with the customer MAC address.
	bmac-mac-address	Static backbone MAC address in hexadecimal format.
Command Default	None	

Command Modes	PBB edge configuration mode
Command History	Release Modification
	Release 3.9.1 This command was introduced.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
Task ID	Task Operations ID
	l2vpn read, write
Examples	The following example shows how to map the customer MAC address with the backbone MAC address:
	<pre>interface GigabitEthernet0/0/0/0.1 l2transport encapsulation dot1q 10 ! interface GigabitEthernet0/0/0/0.2 l2transport encapsulation dot1q 2 ! interface GigabitEthernet0/0/0/1 shutdown</pre>
	! interface GigabitEthernet0/0/0/2 shutdown
	! interface GigabitEthernet0/0/0/3 shutdown
	! interface GigabitEthernet0/0/0/4 shutdown !
	l2vpn bridge group bg12 bridge-domain bd1
	interface GigabitEthernet0/0/0.1 static-mac-address 0002.0003.0004 !
	interface GigabitEthernet0/0/0/0.2 ! pbb edge i-sid 1000 core-bridge bd2
	static-mac-address 0006.0007.0008 bmac 0004.0005.0006 !
	end !
	The following example shows the output of the show l2vpn bridge-domain command:
	##sh l2vpn bridge-domain m mac-address mroute

Mac Address	Туре	Learned from/	LC learned	Mapped to

Fil	tered on	1	Resync Age			
0002.0003.0004 st	atic Gi	L0/0/0/0.1		N/A	N/A	N/A
0006.0007.0008 st	atic BD	0 the C		N/A	N/A	0004.0005.0006

Ŵ

Note

To resynchronize the MAC table from the network processors, use the **l2vpn resynchronize** forwarding mac-address-table location < r/s/i > command.

Related Commands

Command	Description	
bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.	
bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.	
pbb, on page 303	Configures the provider backbone bridge core or edge.	
l2vpn, on page 69	Enters L2VPN configuration mode.	
	bridge-domain (VPLS), on page 176 bridge group (VPLS), on page 177 pbb, on page 303	

timers

To configure timers that affect the convergence of PBB EVPN in failure scenarios, use the **timers** command in the EVPN interface configuration or in the EVPN configuration mode. To delete the timer configuration, use the **no** form of this command.

timers [{flushagain | recovery | peering | programming}] no timers [{flushagain | recovery | peering | programming}]

Syntax Description	flushagain	Specifies the MAC flush again timer.	
	recovery	Specifies the recovery timer.	
	peering	Specifies the peering timer.	
	programming	Specifies the programming timer.	
Command Default	None.		
Command Modes	e configuration		
	EVPN configuration		
Command History	Release N	Nodification	
		This command was ntroduced.	

Usage Guidelines To use this command, you must be in a user group associated with a task 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 timers are configured globally in the EVPN configuration mode whereas in the EVPN interface configuration mode, the timers are configured per Ethernet.

The keywords **peering** and **programming** are supported only in the EVPN configuration mode.

 Task ID
 Task
 Operation

 ID
 12vpn
 read,

write

This example shows how to configure timers in the EVPN Interface 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)# timers RP/0/RSP0/CPU0:router(config-evpn-ac-timers)#

This example shows how to configure timers in the EVPN configuration mode:

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

Related Commands	Command	Description
	evpn, on page 289	Enters EVPN configuration mode.
	interface (EVPN), on page 296	Enters the EVPN Interface configuration mode.
	recovery, on page 307	Configures the recovery timer.
	flushagain, on page 291	Configures the MAC flushagain timer.
	peering, on page 304	Configures the peering timer.
	programming, on page 306	Configures the programming timer.

unknown-unicast-bmac

To configure the unknown unicast backbone MAC address for a PBB edge bridge, use the **unknown-unicast-bmac** command in the PBB edge configuration mode. To return to the default behavior, use the **no** form of this command.

unknown-unicast-bmac mac-address no unknown-unicast-bmac mac-address

Syntax Description	mac-address Unknown unicast backbone MAC address in hexadecimal format.		
Command Default	None		
Command Modes	PBB edge con	figuration	
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 Operat ID	ions	
	l2vpn read, write		
Examples	The following PBB edge brid		e the unknown unicast backbone MAC address for a
	interf ! interf ! pbb ed	oup PBB Romain PBB-EDGE Face GigabitEthernet0/0/0/38 Face GigabitEthernet0/2/0/30 Rge i-sid 1000 core-bridge F Rown-unicast-bmac 0123.8888.	.150 BB-CORE
Related Commands	Command	Daga	iption

	•
bridge-domain (VPLS), on page 176	Establishes a bridge domain, and enters L2VPN bridge group bridge domain configuration mode.
bridge group (VPLS), on page 177	Creates a bridge group so that it can contain bridge domains and then to assign network interfaces to the bridge domain.
l2vpn, on page 69	Enters L2VPN configuration mode.
pbb, on page 303	Configures the provider backbone bridge core or edge.



Multiple Spanning Tree Protocol Commands

For detailed information about MSTP concepts, configuration tasks, and examples, see the

Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.

- bridge-id, on page 337
- bringup delay, on page 339
- clear ethernet mvrp statistics, on page 340
- cost, on page 341
- debug ethernet mvrp packets, on page 343
- debug ethernet mvrp protocol, on page 344
- debug spanning-tree mst packet, on page 345
- debug spanning-tree mst protocol-state, on page 347
- debug spanning-tree mstag packet, on page 348
- debug spanning-tree packet raw, on page 349
- debug spanning-tree pvrst, on page 351
- debug spanning-tree pvrstag packet, on page 352
- debug spanning-tree pvstag packet, on page 354
- debug spanning-tree repag packet, on page 355
- edge-mode, on page 356
- external-cost (MSTAG/REPAG), on page 357
- external-cost (MSTP), on page 358
- flush containment disable, on page 359
- forward-delay, on page 360
- forward-delay (PVRST), on page 361
- guard root, on page 362
- guard topology-change, on page 363
- hello-time (Access Gateway), on page 364
- hello-time (MSTP), on page 366
- instance (MSTAG/REPAG), on page 367
- instance (MSTP), on page 368
- instance cost, on page 369
- instance port-priority, on page 370
- interface (MSTAG/REPAG), on page 371
- interface (MSTP), on page 373
- interface (PVRST), on page 374

- interface (PVSTAG/PVRSTAG), on page 375
- interface (MSTAG Uplink Tracking), on page 376
- join-time, on page 378
- leave-time, on page 379
- leaveall-time, on page 380
- link-type, on page 381
- max age, on page 382
- maximum (PVRST), on page 384
- maximum age, on page 385
- maximum hops (MSTP), on page 386
- mvrp static, on page 387
- name (MSTAG/REPAG), on page 388
- name (MSTP), on page 389
- periodic transmit, on page 390
- port-id, on page 391
- port-priority, on page 393
- portfast, on page 395
- preempt delay, on page 396
- priority (Access Gateway), on page 397
- priority (MSTP), on page 398
- provider-bridge (MSTAG/REPAG), on page 399
- provider-bridge (MSTP), on page 400
- revision (MSTAG/REPAG), on page 401
- revision (MSTP), on page 402
- root-cost, on page 403
- root-id, on page 405
- root-priority, on page 407
- show ethernet mvrp mad, on page 409
- show ethernet mvrp statistics, on page 410
- show ethernet mvrp status, on page 411
- show l2vpn mstp port, on page 412
- show l2vpn mstp vlan, on page 414
- show spanning-tree mst, on page 415
- show spanning-tree mst bpdu interface, on page 417
- show spanning-tree mst configuration, on page 419
- show spanning-tree mst errors, on page 420
- show spanning-tree mst interface, on page 421
- show spanning-tree mst topology-change flushes, on page 424
- show spanning-tree mstag, on page 426
- show spanning-tree mstag bpdu interface, on page 428
- show spanning-tree mstag topology-change flushes, on page 429
- show spanning-tree mstag tracked, on page 431
- show spanning-tree pvrst, on page 432
- show spanning-tree pvrstag, on page 435
- show spanning-tree pvstag, on page 436
- show spanning-tree repag, on page 438

L

- show spanning-tree repag bpdu interface, on page 439
- show spanning-tree repag topology-change flushes, on page 441
- spanning-tree mst, on page 443
- spanning-tree mstag, on page 444
- spanning-tree pvrst, on page 445
- spanning-tree pvrstag, on page 446
- spanning-tree pvstag, on page 447
- spanning-tree repag, on page 448
- track, on page 449
- transmit (PVRST), on page 450
- transmit hold-count, on page 451
- vlan, on page 452
- vlan (PVRST), on page 453
- vlan-ids (MSTAG/REPAG), on page 454
- vlan-id (MSTP), on page 455

bridge-id

To set the bridge ID for this device for an Access Gateway instance, use the **bridge-id** command in MSTAG interface configuration, REPAG Interface configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

bridge-id id [startup-value startup-id]

Syntax Description	id	MAC address of the switch. It can be any 48-bit value.			
	startup-value	startup-value Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.			
	startup-id	Sets the startup bridge ID.			
Command Default	For MSTAG/R	EPAG, the MAC address of the switch. For PVSTAG/PVRSTAG, the interface MAC address.			
	If no startup va	lue is specified, the normal value is used during startup.			
Command Modes	MSTAG interface configuration, REPAG Interface configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration				
Command History	Release	Modification			
	Release 3.7.1	This command was introduced.			
	Release 4.0.0	This command was supported in the PVSTAG VLAN configuration and PVRSTAG VLAN configuration submodes.			
Usage Guidelines		nmand, you must be in a user group associated with a task group that includes appropriate task group assignment is preventing you from using a command, contact your AAA administrator			

Task ID	Task ID	Operations
	interface (for MSTAG/REPAG)	read, write
	ethernet-services (for PVSTAG/PVRSTAG) read, write
Examples	The following example shows how to set the	e bridge ID:
	RP/0/RSP0/CPU0:router(config-mstag-if	E) # bridge-id 001c.0000.0011
Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	debug spanning-tree pvrstag packet, on page 352	Enables packet debugging for sent and received PVRSTAG packets.
	debug spanning-tree pvstag packet, on page 354	Enables packet debugging for sent and received PVSTAG packets
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface (MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	interface (PVSTAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
	spanning-tree pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
	spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.

When configuring access gateway, this command is used to modify the value of the bridge ID that is advertised in the STP BPDUs.

Command	Description	
show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.	
vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.	

bringup delay

I

To configure a delay when an interface is first created before it is added to the MSTP topology, use the **bringup delay** command in the MSTP configuration mode.

	bringup delay for <i>interval</i> {seconds minutes hours} no bringup delay for <i>interval</i> {seconds minutes hours}		
Syntax Description	<i>interval</i> Length of time to delay adding the interface to the MSTP topology.		
	seconds Specifies the delay in seconds.		
	minutes Specifies the delay in minutes.		
	hours Specifies the delay in hours.		
Command Default	If no bringup delay is configured, interfaces are added to the MSTP topology as soon as they are created.		
Command Modes	MSTP configuration		
Command History	Release Modification		
	Release 3.9.1 This command was introduced.		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
	This command is used to change the behaviour of MSTP when interfaces are first functional (for example, when a line card boots for the first time). By default, interfaces are added to the MSTP topology, and may be placed in the forwarding state, as soon as the system declares that the interfaces are functional. However, at this point the data plane may not be fully prepared to forward traffic on the interface. If a bringup delay is configured, MSTP keeps the interface in blocked state for the specified delay, and adds it to the MSTP topology only after the specified interval has occurred.		
	For information on configuring bringup delay, refer to the Implementing Multiple Spanning Tree Protocol module of the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.		

Task ID	Task ID	Operations		
	interface	read, write		
Examples	The following example shows how to configure the bringup delay:			
Related Commands	RP/0/RS	SPO/CPU0:router# configure SPO/CPU0:router(config)#spanning- SPO/CPU0:router(config-mstp)# bri		
			•	
	debug	spanning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.	
	debug spanning-tree mst protocol-state, on page 347		Enables debugging protocol-state changes such as port role or state changes, topology change notification.	
	spannir	ng-tree mst, on page 443	Enters the MSTP configuration submode	
	show s	panning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.	

clear ethernet mvrp statistics

To clear MVRP statistics for ethernet interfaces, use the **clear ethernet mvrp statistics** command in the EXEC mode.

clear ethernet mvrp statistics {interface type interface-path-id | location | all}

Syntax Description	interface	(Optional) Clears the MVRP statistics for the given interface.				
	type	Interface type. For more information, use the question mark (?) online help function.				
	interface-path-id	interface-path-id Physical interface or virtual interface.				
			Use the show interfaces command to see a list of all interfaces currently configured on the router.			
		For more help funct	information about the syntax for the router, use the question mark (?) online ion.			
	location	Clears M	VRP statistics for interfaces in a particular location.			
	location	Specifies the fully qualified location.				
	all	Clears the MVRP statistics for all interfaces.				

Command Default None

Command Modes	EXEC		
Command History	Release	Modification	
	Release 3.9.1	This command was introduced.	
Usage Guidelines		er group assignment is preventing	oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task ID	Operations	
	ethernet-servi	ces execute	
Examples	The following	g example shows how to configu	re the bringup delay:
	RP/0/RSP0/C	PU0:router# clear ethernet r	nvrp statistics all
Related Commands	Command		Description
	mvrp static, o	on page 387	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
	show ethern	et mvrp statistics, on page 410	Displays packet statistics per port.
cost	instance or R	rnal path cost for a given instance EPAG interface instance configur cartup-value startup-cost]	on the current port, use the cost command in MSTAG interface ration submode.
Syntax Description	cost	Port cost. Range is 1 to 20000	0000.
	startup-value Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.		
	startup-id	Sets the startup internal path co	ost.
Command Default	If the startup	value is not specified, it defaults	to 20000000.
Command Modes	MSTAG interface instance configuration, REPAG Instance Configuration		

Command History	Release	Modification	
	Release 3.7.1	This command was introduced.	_
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
	This comman MSTI in the S		ess Gateway, to change the cost value that is advertised for this
Note		r bundle interfaces is fixed to 1 idual members.	0000 and does not depend on the number of interfaces and the
Task ID	Task ID Op	erations	
	interface rea	ad, ite	
	WI		
Examples	The following	example shows how to set the	-
-	The following	g example shows how to set the	-
	The following RP/0/RSP0/CE Command	g example shows how to set the	-inst)# cost 10000 Description
	The following RP/0/RSP0/CE Command debug spanni 348	g example shows how to set the	-inst)# cost 10000 Description
	The following RP/0/RSP0/CE Command debug spanni 348 debug spanni 355	g example shows how to set the PUO:router(config-mstag-if- ing-tree mstag packet, on page	-inst) # cost 10000 Description Enables MSTAG packet debugging. Enables Resilient Ethernet Protocol (REP) Access Gateway
	The following RP/0/RSP0/CE Command debug spanni 348 debug spanni 355 interface (MS	g example shows how to set the 200:router(config-mstag-if- ing-tree mstag packet, on page ing-tree repag packet, on page	 Description Enables MSTAG packet debugging. Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands. Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
-	The following RP/0/RSP0/CE Command debug spanni 348 debug spanni 355 interface (MS instance (MS	g example shows how to set the PUO:router(config-mstag-if- ing-tree mstag packet, on page ing-tree repag packet, on page STAG/REPAG), on page 371	 Description Enables MSTAG packet debugging. Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands. Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port. Enters MSTAG Instance configuration mode or REPAG Instance
•	The following RP/0/RSP0/CE Command debug spanni 348 debug spanni 355 interface (MS instance (MS spanning-tree	g example shows how to set the 200:router(config-mstag-if- ing-tree mstag packet, on page ing-tree repag packet, on page STAG/REPAG), on page 371 TAG/REPAG), on page 367	 -inst) # cost 10000 Description Enables MSTAG packet debugging. Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands. Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port. Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
Examples	The following RP/0/RSP0/CE Command debug spanni 348 debug spanni 355 interface (MS instance (MS spanning-tree spanning-tree	s example shows how to set the 200:router(config-mstag-if- ing-tree mstag packet, on page ing-tree repag packet, on page STAG/REPAG), on page 371 TAG/REPAG), on page 367 e mstag, on page 444	 Description Enables MSTAG packet debugging. Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands. Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port. Enters MSTAG Instance configuration mode or REPAG Instance configuration mode. Enters the MST Access Gateway configuration submode. Enters the Resilient Ethernet Protocol Access Gateway (REPAG)

debug ethernet mvrp packets

To enable debugging of sent and received MVRP packets, use the **debug ethernet mvrp packets** command in the EXEC mode. To disable debugging, use the **no** form of this command.

debug ethernet mvrp packets {brief | full | hexdump} [direction {received | sent}] [{interface interface-name | location node-id}] no debug ethernet mvrp packets {brief | full | hexdump} [direction {received | sent}] [{interface interface-name | location node-id}]

Syntax Description	brief		Enables	s brief debugging output.
	full		Enables	s full debugging output.
	hexdump		Enables	s full debugging output along with the raw contexts of the packet in hex.
	direction		{Option	nal} Restricts output to a packet direction.
	received	received sent		es packets received.
	sent			es packets sent.
	interface i	interface interface-name		nal} Filters by interface.
			Physica	l interface or a virtual interface.
			Note Use the show interfaces command to see a list of all possible currently configured on the router.	
				For more information about the syntax for the router, use the question mark (?) online help function.
	location no	ode-id		al) Indicates the location. The <i>node-id</i> argument is entered in the ot/module notation.
Command Default	By default,	debugging is e	nabled f	or both directions for all interfaces.
Command Modes	EXEC			
Command History	Release	Modificatio	n	
	Release 4.0.1	This comma introduced.	and was	
Usage Guidelines		user group assig		in a user group associated with a task group that includes appropriate task s preventing you from using a command, contact your AAA administrator
Task ID	Task ID	Operation	ls	
	ethernet-ser	vices read		

.

Examples	The following example shows how to enable debugging of brief MVRP packets: RP/0/RSP0/CPU0:router#debug ethernet mvrp packets brief Thu Oct 28 02:56:35.048 DST					
	The following example shows how to enable debugging of full MVRP packets on a specific location:					
RP/0/RSP0/CPU0:router# debug ethernet mvrp packets full location 0/0/CPU0 Mon Nov 15 20:02:13.636 PST						
	The following example shows how to enable debugging of brief MVRP packets received at a s interface:					
	RP/0/RSP0/CPU0:router#debug ethernet mvrp packets brief direction received interface gigabitEthernet 0/0/0/1 Thu Nov 25 21:09:01.986 PST					
Related Commands	Command	Description				
	debug ethernet mvrp protocol, on page 344	Enables MVRP protocol debugging on a specific interface, location or vlan.				
	mvrp static, on page 387	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.				
	show ethernet mvrp mad, on page 409	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.				
	show ethernet mvrp statistics, on page 410	Displays packet statistics per port.				

debug ethernet mvrp protocol

show ethernet mvrp status, on page 411

To enable MVRP protocol debugging on a specific interface, location or vlan, use the **debug ethernet mvrp** protocol command in the EXEC mode. To disable debugging, use the no form of this command.

Displays a summary of the VIDs that are declared or registered.

debug ethernet mvrp protocol [vlan vlan-id] [{interface interface-name | location node-id}] **no debug ethernet myrp protocol** [vlan vlan-id] [{interface interface-name | location node-id}]

Syntax Description	vlan vlan-id	{Optional} Specific vlan-id to filter on.
	interface	{Optional} Filters by interface.
	interface-name	Physical interface or a virtual interface.
		Note Use the show interfaces command to see a list of all possible interfaces currently configured on the router.
		For more information about the syntax for the router, use the question mark (?) online help function.

	location <i>n</i>	ode-id	(Optional) Indicate rack/slot/module n	es the location. The <i>node-id</i> argument is entered in the notation.	
Command Default	By default,	debug is enab	bled for all vlans, in	terfaces, and locations.	
Command Modes	EXEC				
Command History	Release	Modificatio	on	-	
	Release 4.0.1	This comm introduced		-	
Usage Guidelines		user group ass		group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator	
Task ID	Task ID	Operatio	ins		
	ethernet-set	rvices read			
Examples	The following example shows how to debug an ethernet mvrp protocol:				
	RP/0/RSP0/CPU0:router# debug ethernet mvrp protocol Thu Oct 28 03:05:21.575 DST				
	RP/0/RSP0/CPU0:router# debug ethernet mvrp protocol location 0/0/CPU0 Mon Nov 15 20:11:56.607 PST				
		/CPU0:router 5 20:12:49.7	-	mvrp protocol interface gigabitEthernet 0/0/0/1	
Related Commands	Command			Description	
	debug eth	ernet mvrp pa	ckets, on page 343	Enables debugging of sent and received MVRP packets.	
	mvrp statio	c, on page 387		Enables Multiple VLAN Registration Protocol (MVRP) in static mode.	
	show ethe	rnet mvrp mac	d, on page 409	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.	
	show ethe	rnet mvrp stat	istics, on page 410	Displays packet statistics per port.	
	show ethe	rnet mvrp stat	us, on page 411	Displays a summary of the VIDs that are declared or registered.	

debug spanning-tree mst packet

To enable debugging for sent and received MSTP packets, use the **debug spanning-tree mst packet** command in the EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree mst packet {brief | full} {sent | received} [interface interface-name] no debug spanning-tree mst packet {brief | full} {sent | received} [interface interface-name]

Suntay Decariation						
Syntax Description	brief	Enables brief debugging output.				
	full	Enables full debugging output.				
	sent Display packets being sent.					
	received	Display packets being received.				
	interface	{Optional} Filters by interface.				
	interface-name	Physical interface or a virtual interface.				
		Note Use the show interfaces command to see a list of all possible interfaces currently configured on the router.				
		For more information about the syntax for the router, use the question mark (?) online help function.				
Command Default	If an interface is not a	specified, then debug is enabled for all interfaces.				
Command Modes	EXEC					
Command History	Release Modifie	cation				
	ReleaseThis co4.0.1introdu	ommand was aced.				
Usage Guidelines		, you must be in a user group associated with a task group that includes appropriate task assignment is preventing you from using a command, contact your AAA administrator				
Task ID	Taalu ID Onevetieve	_				
	Task ID Operations					
	interface read	-				
	interface read	- - ble shows how to enable brief debugging for received packets:				
	interface read	- - ple shows how to enable brief debugging for received packets: ater#debug spanning-tree mst packet brief received				
Examples	interface read The following examp RP/0/RSP0/CPU0:rou Mon Nov 15 20:42:5	- - ple shows how to enable brief debugging for received packets: ater#debug spanning-tree mst packet brief received				
	interface read The following examp RP/0/RSP0/CPU0:rou Mon Nov 15 20:42:5 The following examp location:	- ole shows how to enable brief debugging for received packets: nter# debug spanning-tree mst packet brief received 58.584 PST				
	interface read The following examp RP/0/RSP0/CPU0:rou Mon Nov 15 20:42:5 The following examp location:	- ble shows how to enable brief debugging for received packets: hter#debug spanning-tree mst packet brief received 58.584 PST ble shows how to enable brief debugging for received packets at a specific hter#debug spanning-tree mst packet brief received location 0/0/CPU0				

RP/0/RSP0/CPU0:router#debug spanning-tree mst packet brief received interface gigabitEthernet
 0/0/0/1
Mon Nov 15 20:45:40.047 PST

Related Commands	Command	Description
	debug spanning-tree mst protocol-state, on page 347	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	debug spanning-tree packet raw, on page 349	Enables debugging raw packet output for all received packets or sent packets.
	spanning-tree mst, on page 443	Enters the MSTP configuration submode
	show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.

debug spanning-tree mst protocol-state

To enable debugging protocol-state changes such as port role or state changes, topology change notification, use the **debug spanning-tree mst protocol-state** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree mst protocol-state [instance instance-id] [interface interface-name] **no debug spanning-tree mst protocol-state** [instance instance-id] [interface interface-name]

Syntax Description	instance <i>instance-id</i> View debug for a specific MSTI.		
	interface interface-name	View debug for a specific interface.	
Command Default	If no instance or interfa	ice is specified, debug is enabled for all	instances and interfaces.
Command Modes	EXEC		
Command History	Release Modifica	tion	
	ReleaseThis com4.0.1introduce	nmand was ed.	
Usage Guidelines			vith a task group that includes appropriate task g a command, contact your AAA administrator
Task ID	Task ID Operations		
	interface read		

Examples	The following example shows how to enable protocol state debugging:				
	RP/0/RSP0/CPU0:router# debug spanning-tree mst protocol-state Mon Nov 15 20:53:52.793 PST				
	RP/0/RSP0/CPU0:router# debug spanning-tree mst protocol-state interface gigabitEthernet 0/0/0/1 Mon Nov 15 20:54:57.310 PST				
	RP/0/RSP0/CPU0:router# debug spanning-tree mst protocol-state instance 4094 Mon Nov 15 20:59:35.860 PST				
Deleted Opposite					

Related Commands	Command	Description	
	debug spanning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.	
	spanning-tree mst, on page 443	Enters the MSTP configuration submode	
	show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.	

debug spanning-tree mstag packet

To enable MSTAG packet debugging, use the debug spanning-tree mstag packet command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree mstag packet {brief | full} {sent | received} [interface interface-name] no debug spanning-tree mstag packet {brief | full} {sent | received} [interface interface-name]

Syntax Description	brief	Enables brief debugging output.		
	full	Enables full debugging output.		
	received	Display packets being received.		
	sent Display packets being sent.	Display packets being sent.		
	interface interface-name	{Optional} Filters by interface.		
		Physical interface or a virtual interface.		
		Note Use the show interfaces command to see a list of all possible interfaces currently configured on the router.		
		For more information about the syntax for the router, use the question mark (?) online help function.		
	If the interface is not	t specified, the debug is enabled for all interfaces.		
Command Modes	EXEC			

Command History	Release	Modifi	cation			
	Release 4.0.1	This co introdu	ommand was ced.			
Usage Guidelines		e user group		oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator		
Task ID	Task ID	Operations				
	interface	read				
Examples	The following example shows how to enable MSTAG packet debugging:					
	RP/0/RSP0/CPU0:router# debug spanning-tree mstag packet brief received Mon Nov 15 21:11:30.464 PST					
	0/0/0/1	0/CPU0:rou 15 21:12:2		ree mstag packet full sent interface gigabitEthernet		
Related Commands	Comman	d		Description		
	debug sp	anning-tree	packet raw, on page 349	Enables debugging raw packet output for all received packets or sent packets.		
	spanning	-tree mstag	, on page 444	Enters the MST Access Gateway configuration submode.		
	show spa	anning-tree	mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.		

debug spanning-tree packet raw

To enable debugging raw packet output for all received packets or sent packets, use the **debug spanning-tree packet raw** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree packet raw {sent | received} [interface interface-name] no debug spanning-tree packet raw {sent | received} [interface interface-name]

Syntax Description	received	Display packets being received.
	sent	Display packets being sent.

	interface	{Optional} Filters b	y interface.		
	interface-name	Physical interface of	a virtual interface.		
			ow interfaces command to see a list of all possible interfaces configured on the router.		
		For more informatic online help function	n about the syntax for the router, use the question mark (?).		
Command Default	If an interface is not sp	ecified, debug is enable	ed for all interfaces.		
Command Modes	EXEC				
Command History		ation			
	ReleaseThis con4.0.1introduce	nmand was ed.			
Usage Guidelines		-	oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator		
	This command enables PVRSTAG.	s raw packet debug for a	Ill STP protocols: MSTP, MSTAG, REPAG, PVSTAG and		
Task ID	Task ID Operations				
	interface read				
Examples	The following example shows how to enable debugging raw packet output for packets received at a specific location:				
	RP/0/RSP0/CPU0:rout Mon Nov 15 21:16:42		ree packet raw received location 0/0/CPU0		
	The following example specific interface:	e shows how to enable o	lebugging raw packet output for packets sent from a		
	RP/0/RSP0/CPU0:rout Mon Nov 15 21:17:43		ree packet raw sent interface gigabitEthernet 0/0/0/1		
Related Commands	Command		Description		
	debug spanning-tree r	nst packet, on page 345	Enables debugging for sent and received MSTP packets.		
	debug spanning-tree r 348	nstag packet, on page	Enables MSTAG packet debugging.		

Command	Description
debug spanning-tree pvstag packet, on page 354	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
spanning-tree mst, on page 443	Enters the MSTP configuration submode
spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.

debug spanning-tree pvrst

To enable debugging protocol-state changes such as port role, state changes, and topology change notification, use the debug spanning-tree pvrst command in EXEC mode. To disable debugging, use the no form of this command.

debug spanning-tree pvrst {controller | io | packet | protocol-state} no debug spanning-tree pvrst {controller | io | packet | protocol-state}

Syntax Description	controller Enables Spanning Tree Protocol (STP) controller debugging.			
	io	Enables PVRST IO de	ebugging.	
	packet	packet Enables PVRST packets debugging.		
	protocol-sta	te Enables protocol state	debugging.	-
Command Default	None			
Command Modes	EXEC			
Command History	Release	Modification		
	Release 5.1	This command was introduced.		
Usage Guidelines		er group assignment is pr	a user group associated with a task grou eventing you from using a command, o	1 11 1

Task ID	Task ID Operations
	ethernet-services read
Examples	This example shows how to enable protocol state debugging:
	RP/0/RSP0/CPU0:router# debug spanning-tree pvrst protocol-state RP/0/RSP0/CPU0:router#
	<pre>debug spanning-tree pvrst protocol-state interface gigabitEthernet 0/0/0/1 vlan 400 RP/0/RSP0/CPU0:router#</pre>
	This example shows a sample output for when controller keyword is used:
	This example shows a sample output for when io keyword is used:
	This example shows a sample output for when packet keyword is used:
	This example shows a sample output for when protocol-state keyword is used:

Related Commands	Command	Description	
	spanning-tree pvrst, on page 445	Enters the Per VLAN Rapid Spanning Tree (PVRST) configuration submode.	
	show spanning-tree pvrst, on page 432	Displays the Per VLAN Rapid Spanning Tree (PVRST) status information.	

debug spanning-tree pvrstag packet

To enable packet debugging for sent and received PVRSTAG packets, use the **debug spanning-tree pvrstag packet** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree pvrstag packet {brief | full} {sent | received} [interface interface-name] no debug spanning-tree pvrstag packet {brief | full} {sent | received} [interface interface-name]

Syntax Description	brief	Enables brief debugging output.
	full	Enables full debugging output.
	sent	Indicates packets sent.
	received	Indicates packets received.

	interface <i>interface-name</i>	{Optional} Filter	rs by interface.		
		Physical interfac	e or a virtual interface.		
			e show interfaces command to see a list of all possible interfaces tly configured on the router.		
		For more inform online help funct	ation about the syntax for the router, use the question mark (?) tion.		
Command Default	If an interface is not	specified, then debug	is enabled for all interfaces.		
Command Modes	EXEC				
Command History	Release Modif	ication	—		
	ReleaseThis of4.0.1introd	command was luced.	_		
Usage Guidelines			r group associated with a task group that includes appropriate task ting you from using a command, contact your AAA administrator		
Task ID	Task ID 0	perations			
	ethernet-services de	ebug			
Examples	The following exam a specific interface:	ple shows how to enab	ble packet debugging for PVRSTAG packets received at		
	RP/0/RSP0/CPU0:rc gigabitEthernet (Wed Nov 24 22:12:	0/0/0/1	g-tree pvrstag packet brief received interface		
	The following example shows how to enable packet debugging for PVRSTAG packets sent from a specific interface:				
	<pre>RP/0/RSP0/CPU0:router#debug spanning-tree pvrstag packet brief sent interface gigabitEtherne 0/0/0/1 Wed Nov 24 22:15:12.893 PST</pre>				
Related Commands	Command		Description		
	show spanning-tree	e pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.		
	spanning-tree pvrs	tag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.		

debug spanning-tree pvstag packet

To enable packet debugging for sent and received PVSTAG packets, use the **debug spanning-tree pvstag packet** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree pvstag packet {brief | full} {sent | received} [interface interface-name] no debug spanning-tree pvstag packet {brief | full} {sent | received} [interface interface-name]

Syntax Description	brief	Enables b	rief debugging output.	
	full	Enables fu	all debugging output.	
	sent	Indicates j	packets sent.	
	received	Indicates j	packets received.	
	interface	{Optional	Filters by interface.	
	interface-name	Physical in	nterface or a virtual interface.	
			Use the show interfaces command to see a list of all possible interfaces currently configured on the router.	
		For more information about the syntax for the router, use the question mark (?) online help function.		
Command Default	If an interface is not	specified, then	debug is enabled for all interfaces.	
Command Modes	EXEC			
Command History	Release Modifi	cation		
	ReleaseThis co4.0.1introdu	ommand was uced.		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate tas IDs. If the user group assignment is preventing you from using a command, contact your AAA administrat for assistance.			
Task ID	Task ID Op	erations		
	ethernet-services de	oug		
Examples	The following example shows how to enable packet debugging for PVSTAG packets received at a specific interface:			
	RP/0/RSP0/CPU0:roo gigabitEthernet 0, Wed Nov 24 22:12:	/0/0/1	anning-tree pvstag packet brief received interface	

L

The following example shows how to enable packet debugging for PVSTAG packets sent from a specific interface:

RP/0/RSP0/CPU0:router#debug spanning-tree pvstag packet brief sent interface gigabitEthernet
 0/0/0/1
Wed Nov 24 22:15:12.893 PST

Related Commands	Command	Description
	show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
	spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.

debug spanning-tree repag packet

To enable Resilient Ethernet Protocol (REP) Access Gateway debugging commands, use the **debug spanning-tree repag packet** command in the EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree repag packet {brief | full} {sent | received} [interface interface-name] no debug spanning-tree repag packet {brief | full} {sent | received} [interface interface-name]

Syntax Description	brief	Enables brief debugging output.
	full	Enables full debugging output.
	received	Display packets being received.
	sent	Display packets being sent.
	interface interface-name	{Optional} Filters by interface.
		name Physical interface or a virtual interface.
		Note Use the show interfaces command to see a list of all possible interfaces currently configured on the router.
		For more information about the syntax for the router, use the question mark (?) online help function.
Command Default	If an interfa	ace is not specified, then debug is enabled for all interfaces.
Command Modes	EXEC	
Command History	Release	Modification
	Release 4.0.1	This command was introduced.

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

Task ID Task ID Operations

Examples

The following example shows how to enable brief debug for REP Access Gateway packets received at a specified interface.

RP/0/RSP0/CPU0:router#debug spanning-tree repag packet brief received interface gigabitEthernet 0/0/0/1 Mon Nov 15 21:26:08.155 PST

The following example shows how to enable full debug for REP Access Gateway packets sent from a specific location:

 $\label{eq:RP/0/RSP0/CPU0:router#debug spanning-tree repag packet full sent location 0/0/CPU0 Mon Nov 15 21:27:10.674 PST$

edge-mode

To enable MSTAG edge mode for Multiple Spanning Tree Instance (MSTI), use the **edge-mode** command in MSTAG instance configuration submode. Use the **no** form of this command to disable the MSTAG edge mode.

	edge-mode no edge-mode		
Syntax Description	This command has no keywords or arguments.		
Command Default	Disabled		
Command Modes	MSTAG instanc	e configurat	
Command History	Release N	Aodification	
		This comman ntroduced.	
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate tas IDs. If the user group assignment is preventing you from using a command, contact your AAA administrate for assistance.		
Task ID	Task ID	Operation	
	ethernet-services	read, write	

This example shows the output from the **edge-mode** command:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#spanning-tree mstag A
RP/0/RSP0/CPU0:router(config-mstag)#interface GigabitEthernet 0/2/0/1.1
RP/0/RSP0/CPU0:router(config-mstag-if)#instance 100
RP/0/RSP0/CPU0:router(config-mstag-if-inst)#edge-mode
RP/0/RSP0/CPU0:router(config-mstag-if-inst)#
```

Related Commands

Command	Description
spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.

external-cost (MSTAG/REPAG)

To set the external path cost on the current port, use the **external-cost** command in MSTAG interface or REPAG interface configuration submode.

Syntax Description	cost	Interface external path cost. Range is 1 to 200000000.
	startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
	startup-cost	Sets the external path cost.
Command Default	If no startup-va	lue is configured, the startup value defaults to 200000000.
Command Modes	MSTAG interfa	ace configuration, REPAG Interface Configuration
Command History	Release	Modification
		This command was introduced.
Usage Guidelines		mand, you must be in a user group associated with a task group that includes appropriate task group assignment is preventing you from using a command, contact your AAA administrator
		is used when configuring Access Gateway, to change the external cost that it advertised in ent from this interface.

external-cost cost [startup-value startup-cost]

I

Task ID	Task ID	Operations	
	interface	read, write	
Examples	The follow	ving example shows how to set the	external cost to 10000:
	RP/0/RSP()/CPU0:router(config-mstag-if))# external-cost 10000
Related Commands	Command	1	Description
	debug spa 348	anning-tree mstag packet, on page	Enables MSTAG packet debugging.
	debug spa 355	anning-tree repag packet, on page	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface	(MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	spanning	-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
	spanning	-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
	show spa	nning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spa	nning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.

external-cost (MSTP)

To set the external path cost on the current port, use the **external-cost** command in MSTP interface configuration submode.

	external-cost	cost		
Syntax Description	cost Port cost. Range is 1 to 200000000.			
Command Default	The default pa	th cost depends on the speed	of the link.	
Command Modes	MSTP interfac	ce configuration		
Command History	Release	Modification		
	Release 3.7.1	This command was introduced.		

Usage Guidelines		r group associated with a task group that includes appropriate task ting you from using a command, contact your AAA administrator
Task ID	Task ID Operations	
	interface read, write	
Examples	The following example shows how to set t	he external cost to 10000:
	RP/0/RSP0/CPU0:router:router(config-	mstp-if)# external-cost 10000
Related Commands	Command	Description
	debug spanning-tree mst packet, on page 3	Enables debugging for sent and received MSTP packets.
	debug spanning-tree mst protocol-state, o page 347	n Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	page 547	or state changes, topology change notification.
	interface (MSTP), on page 373	Enters the MSTP interface configuration submode, and enables STP for the specified port.
		Enters the MSTP interface configuration submode, and enables

flush containment disable

To disable the flush containment feature on a bridge, use the **flush containment disable** command in the MSTP configuration submode.

	flush contair	iment disable		
Syntax Description	This command has no keywords or arguments.			
Command Default	Flush containr	Flush containment feature is enabled.		
Command Modes	MSTP configu	iration		
Command History	Release	Modification		
	Release 3.9.1	This command was introduced.		
Usage Guidelines			up associated with a task group that includes appropriate task you from using a command, contact your AAA administrator	

Flush containment is a Cisco feature that helps prevent unnecessary MAC flushes. Refer to the Implementing Multiple Spanning Tree Protocol module in the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.

Task ID	Task ID	Operations	
	interface	read, write	
Examples	The follo	owing example shows how to disable t	he flush containment feature on a bridge:
	RP/0/RS	P0/CPU0:router(config-mstp)# flu	sh containment disable
Related Commands	RP/0/RS		sh containment disable Description
Related Commands	Comma		
Related Commands	Comma debug s	nd panning-tree mst packet, on page 345 panning-tree mst protocol-state, on	Description
Related Commands	Comma debug s debug s page 34	nd panning-tree mst packet, on page 345 panning-tree mst protocol-state, on	Description Enables debugging for sent and received MSTP packets. Enables debugging protocol-state changes such as port role

forward-delay

To set the forward-delay parameter for the bridge, use the forward-delay command in MSTP configuration submode.

	forward-delay	y seconds
Syntax Description	seconds Brid	lge forward delay time in seconds. Range is 4 to 30.
Command Default	seconds: 15	
Command Modes	MSTP configu	iration
Command History	Release	Modification
	Release 3.7.1	This command was introduced.
Usage Guidelines		mmand, you must be in a user group associated with r group assignment is preventing you from using a c

a task group that includes appropriate task command, contact your AAA administrator for assistance.

I

Task ID	Task ID	Operations		
	interface	read, write		
Examples	The follo	wing example s	hows how to set the fo	prward-delay parameter for the bridge to 20:
	RP/0/RSF	0/CPU0:router	(config-mstp)# for	ward-delay 20
Related Commands	Comman	d		Description
	debug sp	oanning-tree ms	t packet, on page 345	Enables debugging for sent and received MSTP packets.
		panning-tree ms	t packet, on page 345 t protocol-state, on	Enables debugging for sent and received MSTP packets. Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	debug sp page 347	panning-tree ms	t protocol-state, on	Enables debugging protocol-state changes such as port role

forward-delay (PVRST)

To set the forward-delay time for the bridge, use the forward-delay command in PVRST configuration submode. To undo the setting, use the no form of this command.

forward-delay seconds no forward-delay seconds

Syntax Description seconds Bridge forward delay time in seconds. The range is from 4 to 30.

None **Command Default**

PVRST configuration **Command Modes**

Command History	Release	Modification	
	Release	This command was	
	5.1	introduced.	

Usage Guidelines

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

I

Task ID	Task ID	Operations				
	ethernet-services	read, write				
Examples	This example shows how to set the forward-delay parameter for the bridge to 20:					
			<pre>spanning-tree pvrst st1 vrst)# forward-delay 20</pre>			
Related Commands	Command		Description			
	interface (PVRS	T), on page 374	Enables and configures Per VLAN Rapid Spanning Tree (PVRST) on an interface.			
	maximum (PVRS	ST), on page 384	Sets the maximum age for the bridge.			
	transmit (PVRS)	Γ), on page 450	Sets the transmit hold count performance parameter.			
	vlan (PVRST), or	n page 453	Configures Per VLAN Rapid Spanning Tree (PVRST) on a VLAN.			

guard root

To prevent a port from becoming the root port for the switch, use the **guard root** command in MSTP interface configuration submode.

	guard root		
Syntax Description	This command has no keywords or arguments.		
Command Default	RootGuard is	disabled.	
Command Modes	MSTP interfac	ce configuration	
Command History	Release	Modification	-
	Release 3.7.1	This command was introduced.	-
Usage Guidelines		r group assignment is preventing	roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
	port. This feat information of	ture can be used to enforce the lo n guard root feature, refer to the	e on the interface, by preventing the port from becoming a root ocation of the root bridge within the MSTP network. For more <i>Implementing Multiple Spanning Tree Protocol</i> module in the <i>Router L2VPN and Ethernet Services Configuration Guide</i> .

Task ID	Task ID	Operations				
	interface	read, write				
Examples	The following example shows how to enable RootGuard on the port:					
	RP/0/RSP0)/CPU0:router(config-mstp-if)#	guard root			
Related Commands	Command	i	Description			
	debug spa	anning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.			
	debug spa page 347	anning-tree mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.			
	interface	(MSTP), on page 373	Enters the MSTP interface configuration submode, and enables STP for the specified port.			
	spanning	-tree mst, on page 443	Enters the MSTP configuration submode			
	show spa	nning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.			

guard topology-change

To enable topology change guard on the port, use the **guard topology-change** command in MSTP interface configuration submode.

	guard topology-change			
Syntax Description	This command has no keywords or arguments.			
Command Default	TopologyChangeGuard is disabled.			
Command Modes	MSTP interface configuration			
Command History	Release	Modification		
	Release 3.7.1	This command was introduced.		
Ilsano Guidelinos	To use this cor	nmand, you must be in a user grou		

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

This command enables topology change guard (also known as restricted TCN) on this interface. When this feature is enabled, topology changes originating at this interfaces, or received in BPDUs on this interface, are not propagated to the rest of the MSTP network. For more information on guard topology, refer to the

Implementing Multiple Spanning Tree Protocol module in the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.

Task ID	Task ID Operations					
	interface read, write					
Examples	The following example shows how to enable TopologyChangeGuard on the port:					
	RP/0/RSP0/CPU0:rou	<pre>iter(config-mstp-if)#</pre>	guard topology-change			
Related Commands	Command		Description			
	debug spanning-tree	mst packet, on page 345	Enables debugging for sent and received MSTP packets.			
	debug spanning-tree page 347	e mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.			
	interface (MSTP), on	page 373	Enters the MSTP interface configuration submode, and enables STP for the specified port.			
	spanning-tree mst, o	n page 443	Enters the MSTP configuration submode			
	show spanning-tree	mst, on page 415	Displays the multiple spanning tree protocol status information.			

hello-time (Access Gateway)

To configure the frequency of sending BPDUs on this interface, use the **hello-time** command in MSTAG interface configuration, REPAG Interface configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

hello-time see	conds
seconds Helle 2.	o time in seconds. Range is 1 to
seconds: 2	
MSTAG interf VLAN configu	face configuration, REPAG Interface configuration, PVSTAG VLAN configuration, PVRSTAG uration
Release	Modification
Release 3.7.1	This command was introduced.
Release 4.0.0	This command was supported in the PVSTAG VLAN configuration and PVRSTAG VLAN configuration mode.
	seconds Hell 2. seconds: 2 MSTAG interf VLAN config Release Release 3.7.1

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

Task ID	 Task ID	Operations
	interface (for MSTAG/REPAG)	read, write
	ethernet-services (for PVSTAG/PVRSTA	G) read, write
Examples	The following example shows how to set th	e port hello time to 1:
	RP/0/RSP0/CPU0:router(config-mstag-i:	f)# hello-time 1
Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	debug spanning-tree pvrstag packet, on page 352	Enables packet debugging for sent and received PVRSTAG packets.
	debug spanning-tree pvstag packet, on page 354	Enables packet debugging for sent and received PVSTAG packets.
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface (MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	interface (PVSTAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
	spanning-tree pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
	spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.

I

Command	Description
show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

hello-time (MSTP)

To set the port hello time, use the hello-time command in MSTP interface configuration submode.

	hello-time	e seconds		
Syntax Description		seconds Hello time in seconds. Range is 1 to 2.		
Command Default	seconds: 2	2		
Command Modes	MSTP int	erface config	guration	
Command History	Release	Modifi	cation	-
	Release 3	.7.1 This co introdu	ommand was uced.	-
Usage Guidelines		user group a		roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task ID	Operations		
	interface	read, write		
Examples	The follow	wing exampl	e shows how to set the	port hello time to 1:
	RP/0/RSP	0/CPU0:rout	ter(config-mstp-if)#	hello-time 1
Related Commands	Command	d		Description
	debug sp	anning-tree i	mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug sp page 347	anning-tree	mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.

Command	Description
interface (MSTP), on page 373	Enters the MSTP interface configuration submode, and enables STP for the specified port.
spanning-tree mst, on page 443	Enters the MSTP configuration submode
show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.

instance (MSTAG/REPAG)

To enter MSTAG Instance configuration mode or REPAG Instance configuration mode, use the **instance** command in MSTAG Interface or REPAG Interface configuration mode respectively.

	instance id		
Syntax Description	<i>id</i> MSTI ID 4094.	0. Range is 0 to	
Command Default	None		
Command Modes	MST AG int	erface configuration, I	REPAG interface configuration
Command History	Release	Modification	
	Release 3.7.	1 This command was introduced.	 ;
Usage Guidelines		er group assignment i	in a user group associated with a task group that includes appropriate task s preventing you from using a command, contact your AAA administrator
Note	An instance	ID of 0 represents the	IST for the region.
Task ID	Task Ope ID	erations	
	interface rea wri		
Examples	The followin	g example shows how	v to enter MSTAG Instance configuration submode:

I

RP/0/RSP0/CPU0:router(config-mstag)# instance 101
RP/0/RSP0/CPU0:router(config-mstag-inst)#

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface (MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.

instance (MSTP)

To enter the multiple spanning tree instance (MSTI) configuration submode, use the **instance** command in MSTP configuration submode.

	instance id			
Syntax Description	<i>id</i> MSTI ID. 4094.	Range is 0 to		
Command Default	None			
Command Modes	MSTP configu	iration		
Command History	Release	Modification		
	Release 3.7.1	This command was introduced.		
Usage Guidelines			in a user group associated v s preventing you from using	

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

Note	An instance ID of 0 represents the CIST for the	e region.
Task ID	Task ID Operations	
	interface read, write	
Examples	The following example shows how to enter the	MSTI configuration submode:
	<pre>RP/0/RSP0/CPU0:router(config-mstp)# ins RP/0/RSP0/CPU0:router(config-mstp-inst)</pre>	
Related Commands	Command	Description
	debug spanning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug spanning-tree mst protocol-state, on page 347	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
		Sets the bridge priority for the current MSTI
	priority (MSTP), on page 398	
	priority (MSTP), on page 398 show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.
		Displays the multiple spanning tree protocol status

instance cost

To set the internal path cost for a given instance on the current port, use the **instance cost** command in MSTP interface configuration submode.

	instance id cost cost
Syntax Description	<i>id</i> MSTI ID. Range is 0 to 4094.
	cost Port cost. Range is 1 to 200000000.
Command Default	The default path cost depends on the speed of the link.
Command Modes	- MSTP interface configuration

I

Command History	Release	Modific	ation			
	Release 3.	.7.1 This con introduc		-		
Usage Guidelines		user group as		roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator		
Note	An instanc	e ID of 0 rep	resents the IST for the	region.		
Task ID	Task ID	Operations				
	interface	read, write				
Examples	The following example shows how to set the port cost to 10000 for the instance ID 101:					
Examples	The follow	ving example	shows how to set the	port cost to 10000 for the instance ID 101:		
Examples				port cost to 10000 for the instance ID 101:		
Examples Related Commands)/CPU0:route				
	RP/0/RSP0)/CPU0:route		instance 101 cost 10000 Description		
	RP/0/RSP0 Command debug spa)/CPU0:route	er(config-mstp-if)#	instance 101 cost 10000 Description		
	RP/0/RSP0 Command debug spa debug spa page 347)/CPU0:route	er (config-mstp-if) # st packet, on page 345 nst protocol-state, on	instance 101 cost 10000 Description Enables debugging for sent and received MSTP packets. Enables debugging protocol-state changes such as port role		
	RP/0/RSP0 Command debug spa debug spa page 347 interface)/CPU0:route I anning-tree m	er (config-mstp-if) # st packet, on page 345 nst protocol-state, on age 373	instance 101 cost 10000 Description Enables debugging for sent and received MSTP packets. Enables debugging protocol-state changes such as port role or state changes, topology change notification. Enters the MSTP interface configuration submode, and enables		

instance port-priority

To set the port priority performance parameter for the MSTI, use the **instance port-priority** command in MSTP interface configuration submode.

	instance	ce id port-priority priority		
Syntax Description	id	MSTI ID. Range is 0 to 4094.		
	priority	Port priority. Range is 0 to 240 in multiples of 16.		

Command Default	priority: 128		
Command Modes	MSTP interfac	ee configuration	
Command History	Release	Modification	-
	Release 3.7.1	This command was introduced.	-
Usage Guidelines			roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Note	An instance II) of 0 represents the CIST for th	ne region.
Task ID	Task ID Oper	ations	
	interface read write	,	
Examples	The following	example shows how to set the	port priority to 160 for the instance ID 101:
	RP/0/RSP0/CP	U0:router(config-mstp-if)#	instance 101 port-priority 160
Related Commands	Command		Description
	debug spanni	ng-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug spanni page 347	ng-tree mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	interface (MS	TP), on page 373	Enters the MSTP interface configuration submode, and enables STP for the specified port.
	spanning-tree	e mst, on page 443	Enters the MSTP configuration submode
	show spannin	g-tree mst, on page 415	Displays the multiple spanning tree protocol status information.

interface (MSTAG/REPAG)

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

interface {Bundle-Ether | GigabitEthernet | TenGigE} instance.subinterface

Syntax Description	instance.subinterface	Physical interface instance, followed by the subinterface identifier. Naming notation is instance.subinterface, and a period between arguments is required as part of the notation.
		• Replace the instance argument with the following physical interface instance. Naming notation is rack/slot/module/port and a slash between values is required as part of the notation.
		• rack—Chassis number of the rack.
		• slot—Physical slot number of the card.
		• module—Module number. A physical layer interface module (PLIM) is always 0.
		• port—Physical port number of the interface.
		• Replace the subinterface argument with the subinterface value. Range is from 0 through 4095.

Command Default	None			
Command Modes	MSTAG configuration, REPAG configuration			
Command History	Release Modification			
	Release 3.7.1 This command was introduced.			
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.			
	The specified subinterface must be configured to match untagged packets, i.e., it must be configured with encapsulation untagged . Only a single subinterface on any given port may be specified.			
	A given port may only be enabled with one of MSTP, MSTAG, REPAG, PVSTAG or PVRSTAG.			
Task ID	Task ID Operations			
	interface read, write			
Examples	The following example shows how to enter the MSTAG interface configuration submode:			

RP/0/RSP0/CPU0:router(config-mstag)# interface GigabitEthernet0/2/0/30.1
RP/0/RSP0/CPU0:router(config-mstag-if)#

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.

interface (MSTP)

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

interface {Bundle-Ether | GigabitEthernet | TenGigE} instance

Syntax Description	instance 1	<i>instance</i> Forward interface in rack/slot/instance/port format.					
Command Default	None						
Command Modes	MSTP con	figuration					
Command History	Release	Modifi	ication				
	Release 3.	7.1 This controduction	ommand was uced.				
Usage Guidelines		user group	you must be in a user assignment is prevent		-	-	
	A given po	rt may only	y be enabled with one	of MSTP, MSTA	AG, REPAG, I	VSTAG or PV	RSTAG.
Task ID	Task ID	Operations					
	interface	read, write					

Examples The following example shows how to enter the MSTP interface configuration submode:

RP/0/RSP0/CPU0:router(config-mstp)# interface GigabitEthernet 0/0/0/1
RP/0/RSP0/CPU0:router(config-mstp-if)#

Related Commands	Command	Description	
	debug spanning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.	
	debug spanning-tree mst protocol-state, on page 347	Enables debugging protocol-state changes such as port role or state changes, topology change notification.	
	spanning-tree mst, on page 443	Enters the MSTP configuration submode	
	show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.	

interface (PVRST)

To enable and configure Per VLAN Rapid Spanning Tree (PVRST) on an interface, use the **interface** command in PVRST configuration mode. To disable PVRST, use the **no** form of this command.

interface {Bundle-Ether | FastEthernet | FortyGigE | GigabitEthernet | HundredGigE | TenGigE][{guard | hello-time | link-type | portfast | vlan }] no interface {Bundle-Eher | FastEthernet | FortyGigE | GigabitEthernet | HundredGigE | TenGigE][{guard | hello-time | link-type | portfast | vlan }]

Syntax Description	Bundle-Ether	Specifies Aggregated Ethernet interface.
	FastEthernet	Specifies FastEthernet/IEEE 802.3 interface.
	FortyGigE	Specifies FortyGigabitEthernet or IEEE 802.3 interface.
	GigabitEthernet	Specifies GigabitEthernet or IEEE 802.3 interface.
	HundredGigE	Specifies HundredGigabitEthernet or IEEE 802.3 interface.
	TenGigE	Specifies TenGigabitEthernet or IEEE 802.3 interface.
	guard	Specifies bridge guard features.
	hello-time	Specifies Hello-Time interface.
	link-type	Specifies the link type of an interface.
	portfast	Specifies Portfast for an interface.
	vlan	Specifies VLAN configuration for an interface.

Command Default None

VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers, IOS XR Release 6.4.x

Command Modes	PVRST cont	PVRST configuration			
Command History	Release	Modification			
	Release 5.1	This command was introduced.			
Usage Guidelines		ser group assignment is pre	user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator		
Task ID	Task ID	Operations			
	ethernet-ser	vices read, write			
Examples	This exampl	e shows how to enter the P	VRST Interface configuration mode:		
	RP/0/RSP0/0	CPU0:router(config)# sg CPU0:router(config-pvrs CPU0:router(config-pvrs	st) # interface GigabitEthernet 0/0/0/1		
Related Commands	Command		Description		
	forward-del	ay (PVRST), on page 361	Sets the forward-delay time for the bridge.		
	maximum (F	PVRST), on page 384	Sets the maximum age for the bridge.		
	transmit (PV	/RST), on page 450	Sets the transmit hold count performance parameter.		
	vlan (PVRS1	F), on page 453	Configures Per VLAN Rapid Spanning Tree (PVRST) on a VLAN.		

interface (PVSTAG/PVRSTAG)

To enter PVST or PVRST Access Gateway Interface configuration submode and to enable either PVSTAG or PVRSTAG for the specified port, use the **interface** command in PVST and PVRST Access Gateway configuration submode.

 interface
 {GigabitEthernet | TenGigE}
 instance

 Syntax Description
 instance
 Forward interface in rack/slot/instance/port format.

 Command Default
 None

 Command Modes
 PVSTAG and PVRSTAG configuration

Command History	Release	Modification	
	Release 4.0.0	This command was introduced.	
Usage Guidelines			r group associated with a task group that includes appropriate task ting you from using a command, contact your AAA administrator
	A given port n	nay only be enabled with one	e of MSTP, MSTAG, REPAG, PVSTAG or PVRSTAG.
Task ID	Task ID	Operations	
	ethernet-servi	ces read, write	
Examples	The following configuration		r the PVST or PVRST Access Gateway Interface
		U0:router(config-pvstag) U0:router(config-pvstag-	<pre># interface GigabitEthernet 0/0/0/1 if)#</pre>
Related Commands	Command		Description
	debug spanni page 352	ng-tree pvrstag packet, on	Enables packet debugging for sent and received PVRSTAG packets.
	debug spanni page 354	ng-tree pvstag packet, on	Enables packet debugging for sent and received PVSTAG packets.
	show spannir	ng-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
	show spannir	ig-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
	spanning-tree	e pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
	spanning-tree		Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG)
		e pvstag, on page 447	configuration submode.

interface (MSTAG Uplink Tracking)

To enable MSTAG Uplink tracking for the specified port, use the **interface** command in the MSTAG Uplink tracking submode.

interface {Bundle-Ether | GigabitEthernet | TenGigE} instance.subinterface

Syntax Description	instance.sul	binterface		nce, optionally followed by the subinterface identifier. Naming interface, and a period between arguments is required as part
				ce argument with the following physical interface instance. s rack/slot/module/port and a slash between values is required ion.
			• rack—Chassi	s number of the rack.
			• slot—Physica	l slot number of the card.
			• module—Mo always 0.	dule number. A physical layer interface module (PLIM) is
			• port—Physica	al port number of the interface.
			• Replace the subint through 4095.	erface argument with the subinterface value. Range is from 0
Command Default	None			
Command Modes	MSTAG Up	olink Trac	king configuration subm	ode
Command History	Release	Modif	ication	
	Release 6.2.2	This c	ommand was introduced.	
Usage Guidelines		iser group		roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task ID C)perations	-	
	interface r	ead, vrite	-	
Examples	The followi submode:	ng examp	ble shows how to enter th	e MSTAG Uplink tracking interface configuration
	RP/0/RSP0/	CPU0:rou	uter(config-mstag)# t uter(config-mstag-tra uter(config-mstag-tra	ck)# interface GigabitEthernet0/2/0/30.1
Related Commands	Command			Description
	debug spar	nnina-tree	e mstag packet, on page	Enables MSTAG packet debugging.

I

Command	Description	
debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.	
spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.	
spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.	
show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.	
show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.	

join-time

To set the join time for all active ports, use the **join-time** command in the MVRP configuration mode. To return to the default value, use the **no** form of this command.

join-time *interval* no join-time *interval*

Syntax Description	<i>interval</i> Maximum time for the join timer parameter for all active ports. The range is from 100 to 1000. The default value is 200.			
Command Default	The default is 200 milliseconds.			
Command Modes	MVRP configuration			
Command History	Release	Modification		
	Release 3.9.1	This comman introduced.	id was	
Usage Guidelines			ust be in a user group associated with a task group that includes appropriate task ment is preventing you from using a command, contact your AAA administrator	
Task ID	Task ID	Operations		
	ethernet-service	es read, write		
Examples	The following	example show	vs how to configure the join time for active ports:	
	RP/0/RSP0/CPT RP/0/RSP0/CPT		configure onfig)# spanning-tree mst AA	

```
RP/0/RSP0/CPU0:router(config-mstp)# mvrp static
RP/0/RSP0/CPU0:router(config-mvrp)# periodic transmit interval 5
RP/0/RSP0/CPU0:router(config-mvrp)# join-time 200
```

Related Commands	Command	Description
	debug ethernet mvrp packets, on page 343	Enables debugging of sent and received MVRP packets.
	debug ethernet mvrp protocol, on page 344	Enables MVRP protocol debugging on a specific interface, location or vlan.
	mvrp static, on page 387	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
	show ethernet mvrp mad, on page 409	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
	show ethernet mvrp statistics, on page 410	Displays packet statistics per port.
	show ethernet mvrp status, on page 411	Displays a summary of the VIDs that are declared or registered.

leave-time

To set the leave time for all active ports, use the **leave-time** command in the MVRP configuration mode. To return to the default value, use the **no** form of this command.

leave-time interval no leave-time interval

Syntax Description *interval* Minimum time, in seconds, for the leaveall timer parameter for all active ports. The range is from 1 to 90 seconds .

Command Default The default is 30 seconds.

Command Modes MVRP configuration

 Command History
 Release
 Modification

 Release 3.9.1
 This command was introduced.

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

```
    Task ID
    Task ID
    Operations

    ethernet-services
    read,
write
```

Examples	The following example shows how to configure the join time for active ports:			
	RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)# spanning-tree mst AA RP/0/RSP0/CPU0:router(config-mstp)# mvrp static RP/0/RSP0/CPU0:router(config-mvrp)# periodic transmit interval 5 RP/0/RSP0/CPU0:router(config-mvrp)# leave-time 30!			
Related Commands	Command	Description		
	debug ethernet mvrp packets, on page 343	Enables debugging of sent and received MVRP packets.		
	debug ethernet mvrp protocol, on page 344	Enables MVRP protocol debugging on a specific interface, location or vlan.		
	mvrp static, on page 387	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.		
	show ethernet mvrp mad, on page 409	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.		
	show ethernet mvrp statistics, on page 410	Displays packet statistics per port.		
	show ethernet mvrp status, on page 411	Displays a summary of the VIDs that are declared or registered.		

leaveall-time

To set the leave all time for all active ports, use the **leaveall-time** command in the MVRP configuration mode. To return to the default value, use the **no** form of this command.

	leaveall-time no leaveall-ti		
Syntax Description		imum time, in seconds, fo 30 seconds.	or the leaveall timer parameter for all active ports. The range is from
Command Default	The default is	10 seconds.	
Command Modes	MVRP config	uration	
Command History	Release	Modification	
	Release 3.9.1	This command was introduced.	
Usage Guidelines			user group associated with a task group that includes appropriate task venting you from using a command, contact your AAA administrator

Task ID	Task ID	Operations	
	ethernet-services	read, write	
Examples	The following ex	xample shows how to config	ure the join time for active ports:
	RP/0/RSP0/CPU0 RP/0/RSP0/CPU0 RP/0/RSP0/CPU0):router# configure):router(config)# spanni):router(config-mstp)# m):router(config-mvrp)# p):router(config-mvrp)# l	vrp static eriodic transmit interval 5
Related Commands	Command		Description
	debug ethernet	mvrp packets, on page 343	Enables debugging of sent and received MVRP packets.
	debug ethernet	mvrp protocol, on page 344	Enables MVRP protocol debugging on a specific interface, location or vlan.
	mvrp static, on	page 387	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
	show ethernet r	nvrp mad, on page 409	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
	show ethernet r	mvrp statistics, on page 410	Displays packet statistics per port.
	show ethernet r	nvrp status, on page 411	Displays a summary of the VIDs that are declared or registered.

link-type

To set the link type of the port to point-to-point or multipoint, use the **link-type** command in MSTP interface configuration submode.

	link-type {po	oint-to-point multipoint}	
Syntax Description	This command has no keywords or arguments.		
Command Default		lue is derived from the duplex se are considered multipoint.	ting for the link. A full-duplex link is considered point-to-point,
Command Modes	MSTP interfac	ce configuration	
Command History	Release	Modification	
	Release 3.7.1	This command was introduced.	

Usage Guidelines		e user group assignment is preventin	roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator		
Task ID	Task ID	Operations			
	interface	read, write			
Examples	The following example shows how to set the link type of the port to point-to-point:				
	RP/0/RSE RP/0/RSE	20/CPU0:router# configure 20/CPU0:router(config)# spannin 20/CPU0:router(config-mstp)# in 20/CPU0:router(config-mstp-if)#	terface GigabitEthernet 0/3/0/3		
Related Commands	Comman	d	Description		
	debug sp	panning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.		
	debug sp page 347	oanning-tree mst protocol-state, on 1	Enables debugging protocol-state changes such as port role or state changes, topology change notification.		
	interface	e (MSTP), on page 373	Enters the MSTP interface configuration submode, and enables STP for the specified port.		
	spanning	g-tree mst, on page 443	Enters the MSTP configuration submode		
	show sp	anning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.		

max age

To set the maximum age for BPDUs sent on this interface, use the **max age** command in MSTAG interface configuration, REPAG interface configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

	max age seconds
Syntax Description	seconds Maximum age time for the bridge in seconds. Range is 6 to 40.
Command Default	seconds: 20
Command Modes	MSTAG interface configuration, REPAG interface configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration
Command History	Release Modification
	Release 3.7.1 This command was introduced.

I

	Release	Modification		
	Release 4.0.0	This command was supporte modes.	in the PVSTAG VLAN and PVRSTAG VL	AN configuration
Usage Guidelines			group associated with a task group that include ng you from using a command, contact your A	
Task ID	Task ID		Operations	
	ethernet-servi	ces (PVSTAG and PVRSTAC	only) read, write	
	interface (MS	TAG and REPAG only)	read, write	
Examples	-	example shows how to set th	maximum age time for the bridge to 20:	
Related Commands	Command		Description	
		ng-tree mstag packet, on page	Enables MSTAG packet debugging.	
	debug spanni page 352	ng-tree pvrstag packet, on	Enables packet debugging for sent and receiv packets.	ved PVRSTAG
	debug spannir 354	ng-tree pvstag packet, on page	Enables packet debugging for sent and receive	d PVSTAG packets
	debug spanni 355	ng-tree repag packet, on page	Enables Resilient Ethernet Protocol (REP) Acc debugging commands.	cess Gateway
	interface (MS	TAG/REPAG), on page 371	Enter the MSTAG interface configuration subr MSTAG for the specified port.	node, and enables
	interface (PV	STAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Inter submode and enables either PVSTAG or PVRS specified port.	
	spanning-tree	e mstag, on page 444	Enters the MST Access Gateway configuration	on submode.
	spanning-tree	e pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Ac (PVRSTAG) configuration submode.	cess Gateway
	spanning-tree	e pvstag, on page 447	Enters the Per VLAN Spanning Tree Access G configuration submode.	ateway (PVSTAG)
	spanning-tree	e repag, on page 448	Enters the Resilient Ethernet Protocol Access configuration submode.	Gateway (REPAG

I

Command	Description
show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

maximum (PVRST)

To set the maximum age for the bridge, use the **maximum** command in PVRST configuration submode. To undo the setting, use the **no** form of this command.

maximum age seconds no maximum age seconds

Syntax Description	age		Specifies the age of the bridge.
	seconds		Maximum age time for the bridge in seconds. The range is from 6 to 40.
Command Default	None		
Command Modes	PVRST conf	iguration	
Command History	Release	Modification	
	Release 5.1	This command was introduced.	
Usage Guidelines		er group assignment is preve	ser group associated with a task group that includes appropriate task enting you from using a command, contact your AAA administrator
Task ID	Task ID	Operations	
	ethernet-servi	ices read, write	
Examples	This example	e shows how to set the maxim	mum age time for the bridge to 40:

RP/0/RSP0/CPU0:router(config)# spanning-tree pvrst st1
RP/0/RSP0/CPU0:router(config-pvrst)# maximum age 40

Related Commands	Command	Description	
	forward-delay (PVRST), on page 361	Sets the forward-delay time for the bridge.	
	interface (PVRST), on page 374	Enables and configures Per VLAN Rapid Spanning Tree (PVRST on an interface.	
	transmit (PVRST), on page 450	Sets the transmit hold count performance parameter.	
	vlan (PVRST), on page 453	Configures Per VLAN Rapid Spanning Tree (PVRST) on a VLAN.	

maximum age

To set the maximum age parameter for the bridge, use the **maximum age** command in MSTP configuration submode.

	maximum age seconds seconds Maximum age time for the bridge in seconds. Range is 6 to 40.		
Syntax Description			
Command Default	seconds: 20		
Command Modes	MSTP configuration		
Command History	Release Modification		
	Release 3.7.1 This command was introduced.		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
Task ID	Task ID Operations		
	interface read, write		
Examples	The following example shows how to set the maximum age time for the bridge to 40:		

RP/0/RSP0/CPU0:router(config-mstp)# maximum age 40

Related Commands	Command	Description	
	spanning-tree mst, on page 443	Enters the MSTP configuration submode	

maximum hops (MSTP)

To set the maximum hops parameters for the bridge, use the **maximum hops** command in MSTP configuration submode.

maximum hops hops

Syntax Description	hops Maxim	num number of hops for the bridge	in seconds. Range is 6 to 40.
Command Default	hops: 20		
Command Modes	MSTP config	uration	
Command History	Release	Modification	
	Release 3.7.1	This command was introduced.	
Usage Guidelines		er group assignment is preventing	oup associated with a task group that includes appropriate task you from using a command, contact your AAA administrator
Task ID	Task ID Ope	erations	
	interface read wri	·	
Examples	The following	g example shows how to set the m	naximum number of hops for the bridge to 30:
	RP/0/RSP0/C	PU0:router(config-mstp)# max	hops 30
Related Commands	Command		Description
	debug spann	ing-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug spann page 347	ing-tree mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	spanning-tre	e mst, on page 443	Enters the MSTP configuration submode

Command	Description
show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.

mvrp static

To enable Multiple VLAN Registration Protocol (MVRP) in static mode and to enter the MVRP configuration submode, use the **mvrp static** command in the MSTP configuration mode. To return to the default setting, use the **no** form of this command.

mvrp static no mvrp static This command has no keywords or arguments. **Syntax Description** None **Command Default** MSTP configuration **Command Modes Command History** Release Modification Release 3.9.1 This command was introduced. To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. Task ID Task ID Operations ethernet-services read, write **Examples** The following example shows how to enable MVRP static mode: RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config) # spanning-tree mst AA RP/0/RSP0/CPU0:router(config-mstp)# mvrp static RP/0/RSP0/CPU0:router(config-mvrp)# **Related Commands** Command Description Enables debugging of sent and received MVRP packets. debug ethernet mvrp packets, on page 343 Enables MVRP protocol debugging on a specific interface, debug ethernet mvrp protocol, on page 344 location or vlan. Sets the join time for all active ports. join-time, on page 378

Command	Description
leave-time, on page 379	Sets the leave time for all active ports.
leaveall-time, on page 380	Sets the leave all time for all active ports.
periodic transmit, on page 390	Sends periodic Multiple VLAN Registration Protocol Data Unit (MVRPDU) on all active ports.
show ethernet mvrp mad, on page 409	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.
show ethernet mvrp statistics, on page 410	Displays packet statistics per port.
show ethernet mvrp status, on page 411	Displays a summary of the VIDs that are declared or registered.
spanning-tree mst, on page 443	Enters the MSTP configuration submode

name (MSTAG/REPAG)

To set the name of the MSTP region, use the **name** command in MSTAG interface configuration or REPAG interface configuration submode.

	name nam	ne					
Syntax Description	name Stri 227	-	imum of 32 charac	ters conformir	ng to the definition	on of SnmpAd	minString in RFC
Command Default	The MAC a IEEE Std 8		e switch, formatted	d as a text strii	ng using the hex	adecimal repre	sentation specified in
Command Modes	MSTAG in	terface conf	iguration, REPAG	interface conf	iguration		
Command History	Release	Modific	ation				
	Release 3.	7.1 This con introduc					
Usage Guidelines		user group a					ludes appropriate task ur AAA administrator
Task ID	Task ID 0	Operations					
	interface r	ead, vrite					
Examples	The follow	ing example	shows how to set	the name of th	e MSTP region	to leo:	

RP/0/RSP0/CPU0:router(config-mstag-if) # name leo

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface (MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.

name (MSTP)

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

	name name		
Syntax Description	<i>name</i> String of a maximum of 32 characters conforming to the definition of SnmpAdminString in RFC 2271.		
Command Default	The MAC add IEEE Std 802.		as a text string using the hexadecimal representation specified in
Command Modes	MSTP configu	iration	
Command History	Release	Modification	_
	Release 3.7.1	This command was introduced.	_
Usage Guidelines		· •	group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator

Task ID	Task ID Operations	
	interface read, write	
Examples	The following example shows how to set t	he name of the MSTP region to m1:
	<pre>RP/0/RSP0/CPU0:router(config-mstp)#</pre>	name m1
Related Commands	Command	Description
	debug spanning-tree mst packet, on page	345 Enables debugging for sent and received MSTP packets.
	debug spanning-tree mst protocol-state, o page 347	n Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	spanning-tree mst, on page 443	Enters the MSTP configuration submode
	show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.

periodic transmit

To send periodic Multiple VLAN Registration Protocol Data Unit (MVRPDU) on all active ports, use the **periodic transmit** command in the MVRP configuration mode. To return to the default value, use the **no** form of this command.

periodic transmit [interval interval] no periodic transmit [interval interval]

Syntax Description interval interval Sends periodic MVRPDU on all active ports at specified time interval. The range is from 2 to 10 seconds.

Command Default The default is 3 seconds.

Command Modes MVRP configuration

Command History Release Modification

Release 3.9.1 This command was introduced.

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

Sending periodic messages is not required when the state machines operate correctly. The periodic messages are intended purely to cope with a succession of lost new declaration MVRPDUs. In the absence of periodic messages, declarations are re-sent every 10 to 15 seconds in response to the LeaveAll timer expiring.

Task ID	Task ID	Operations					
	ethernet-services	read, write					
Examples	The following example shows how to enable MVRP static mode:						
	RP/0/RSP0/CPU0 RP/0/RSP0/CPU0	:router(config-ms	spanning-tree mst AA				
Related Commands	Command		Description				
	debug ethernet	mvrp packets, on pag	e 343 Enables debugging of sent and received MVRP packets.				
	debug ethernet	mvrp protocol, on pa	ge 344 Enables MVRP protocol debugging on a specific interface, location or vlan.				
	mvrp static, on page 387		Enables Multiple VLAN Registration Protocol (MVRP) in static mode.				
	show ethernet r	nvrp mad, on page 40	 Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port. 				
	show ethernet r	nvrp statistics, on pa	ge 410 Displays packet statistics per port.				
	show ethernet r	nvrp status, on page	Displays a summary of the VIDs that are declared or registered.				

port-id

To set the port ID for the current switch, use the **port-id** command in MSTAG interface configuration, REPAG interface configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

port-id id [startup-value startup-id]

Syntax Description	id	Interface port ID.
		For MSTAG, REPAG and PVRSTAG the allowed range is between 1 to 4095. For PVSTAG the allowed range is between 1 to 255.
	startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
	startup-id	Sets the startup port ID.

Command Default	If a startup value is not specified, it defaults to the normal value.
Commanu Delault	if a startup value is not specifica, it defaults to the normal value.

Command Modes MSTAG interface configuration, REPAG interface configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration

Command History	Release	Modification
Release 3.7.1This command was introduced.Release 4.0.0This command was supported in the PVSTAG V modes.	Release 3.7.1	This command was introduced.
	This command was supported in the PVSTAG VLAN and PVRSTAG VLAN configuration modes.	
Usage Guidelines		nmand, you must be in a user group associated with a task group that includes appropriate task r group assignment is preventing you from using a command, contact your AAA administrator

This command is used when configuring Access Gateway, to set the value of the port ID advertised in BPDUs sent on this interface.

Task ID	Task ID	Operations
	ethernet-services (PVSTAG and PVRSTAG only)	read, write
		read, write

Examples The following example shows how to set the port ID:

RP/0/RSP0/CPU0:router(config-mstag-if) # port-id 111

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	debug spanning-tree pvrstag packet, on page 352	Enables packet debugging for sent and received PVRSTAG packets.
	debug spanning-tree pvstag packet, on page 354	Enables packet debugging for sent and received PVSTAG packets.
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface (MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	interface (PVSTAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.

I

Command	Description
instance (MSTAG/REPAG), on page 367	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

port-priority

To set the port priority performance parameter for the MSTI, use the **port-priority** command in MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration, or PVRSTAG VLAN configuration submode.

	port-priority p	priority [startup-value startup-priority]	
Syntax Description	priority	Port priority. For MSTAG, REPAG and PVRSTAG, the range is between 0 to 40 in multiples of 16. For PVSTAG, the range is between 0 to 255.	
	startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.	
	startup-priority	^b Sets the startup port priority.	
Command Default	If no startup-val	ue is configured, the normal value is used during startup.	
Command Modes	MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration		
Command History	Release I	Modification	
	Release 3.7.1	This command was introduced.	

	Release	Modification			
	Release 4.0.0 This command was supported in the PVSTAG VLAN and PVRSTAG VLAN configuration modes.				
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes a IDs. If the user group assignment is preventing you from using a command, contact your AA for assistance.			• • • • • •	
Task ID	Task ID			Operations	
	ethernet-servi	ces (PVSTAG and PVRSTAC	G only)	read, write	
	interface (MS	TAG and REPAG only)		read, write	
Examples	The following	example shows how to set th	e port p	priority to 1	60:
	RP/0/RSP0/CP	U0:router(config-mstag-i	f-inst)	# port-pr	ciority 160
Related Commands	Command		Descr	iption	
	debug spannir 348	ng-tree mstag packet, on page	Enable	es MSTAG p	acket debugging.
	debug spanni page 352	ng-tree pvrstag packet, on	Enable packet	-	ebugging for sent and received PVRSTAG
	debug spannir 354	ng-tree pvstag packet, on page	Enable	es packet de	bugging for sent and received PVSTAG packets.
	debug spannin 355	ng-tree repag packet, on page		es Resilient ging comma	Ethernet Protocol (REP) Access Gateway ands.
	interface (MS	TAG/REPAG), on page 371			interface configuration submode, and enables ecified port.
	interface (PVS	STAG/PVRSTAG), on page 375	submo		/RST Access Gateway Interface configuration bles either PVSTAG or PVRSTAG for the
	instance (MS	TAG/REPAG), on page 367		MSTAG Insuration mod	stance configuration mode or REPAG Instance de.
	spanning-tree	e mstag, on page 444	Enters	the MST A	ccess Gateway configuration submode.
	spanning-tree	e pvrstag, on page 446			AN Rapid Spanning Tree Access Gateway juration submode.
	spanning-tree	e pvstag, on page 447		the Per VL uration sub	AN Spanning Tree Access Gateway (PVSTAG) mode.

Command	Description	
spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.	
show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.	
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.	
show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.	
show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.	
vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.	

portfast

I

To enable Port Fast on the port, and optionally enable BPDU guard, use the **portfast** command in MSTP interface configuration submode.

	portfast [bpduguard]		
Syntax Description	This command has no keywords or arguments.		
Command Default	PortFast is disabled.		
Command Modes	MSTP interface configuration		
Command History	Release Modification		
	Release 3.7.1 This command was introduced.		
Usage Guidelines	You must disable and re-enable the port for Port Fast configuration to take effect. Use shutdown and no shutdown command (in interface configuration mode) to disable and re-enable the port.		
	This command enables the Port Fast feature (also known as edge port). When this is enabled, MSTP treats the port as an edge port, i.e., it keeps it in forwarding state and does not generate topology changes if the port goes down or comes up. It is not expected to receive MSTP BPDUs on an edge port. BPDU guard is a Cisco extension that causes the interface to be shut down using error-disable if an MSTP BPDU is received. For more information on Port Fast feature, refer to the <i>Implementing Multiple Spanning Tree Protocol</i> module in the <i>Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide</i> .		
Task ID	Task ID Operations		
	interface read, write		

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

RP/0/RSP0/CPU0:router(config-mstp-if)# portfast

RP/0/RSP0/CPU0:router(config-mstp-if)# portfast bpduguard

deben en en instanten et en electre en elect	
debug spanning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.
debug spanning-tree mst protocol-state, on page 347	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
interface (MSTP), on page 373	Enters the MSTP interface configuration submode, and enables STP for the specified port.
spanning-tree mst, on page 443	Enters the MSTP configuration submode
show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.
	debug spanning-tree mst protocol-state, on page 347 interface (MSTP), on page 373 spanning-tree mst, on page 443

preempt delay

To enable topology control and set the preempt delay on startup, use the **preempt delay** command in MSTAG, REPAG, PVSTAG or PVRSTAG configuration mode.

	preempt delay {for <i>time</i> {seconds minutes hours} until <i>hh</i> : <i>mm</i> : <i>ss</i> }		
Syntax Description	for Specifies length of time to delay preempting for in seconds, minutes or hours.		
	until Specifies time to delay preempting until the mentioned interval (24-hour hh:mm:ss).		
Command Default	Startup topology control is disabled.		
Command Modes	MSTAG configuration, REPAG configuration, PVSTAG configuration, PVRSTAG configuration		
Command History	Release Modification		
	Release 3.7.1 This command was introduced.		
	Release 4.0.0 This command was supported in the PVSTAG and PVRSTAG configuration modes.		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
	This command enables startup topology control for Access Gateway. By default, when an interface comes up, Access Gateway starts sending STP BPDUs immediately based on the configured values. This could cause the devices in the access network to immediately start directing traffic to this device. However, the data plane may not yet be ready to forward packets to the core or aggregation network. When a preempt delay is		

configured, alternative values are sent in the BPDUs for the specified time. These alternative values must be configured using the **startup-value** option, and can be set so as to cause the access devices not to use this link unless it is the only one available.

For more information on preempt delay, refer to the *Implementing Multiple Spanning Tree Protocol* module in the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide.

Task ID	Task ID	Operations	
	ethernet-services (PVSTAG and PVRSTA	G only) read, write	
	interface (MSTAG and REPAG only)	read, write	
Examples	The following example shows how to set the	e preempt delay for 20 seconds:	
	RP/0/RSP0/CPU0:router(config-mstag)#	preempt delay for 20 seconds	
Related Commands	Command	Description	
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.	
	spanning-tree pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.	'
	spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVS) configuration submode.	AG)
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (RE configuration submode.	PAG)
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs by all ports.	sent
	show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs by all ports.	sent
	show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs by all ports.	sent
	show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs by all ports.	sent

priority (Access Gateway)

To set the bridge priority for the current MSTI or VLAN, use the **priority** command in the MSTAG, REPAG, PVSTAG or PVRSTAG instance configuration submodes.

priority priority [startup-value startup-priority]

neidleu collillidlids	Command		escription nters the MST Access Gateway configuration submode.		
Related Commands	<u> </u>		t)# priority 4096 startup-value 32768		
Examples	The following e	xample shows how to set the brid	ge priority for the current MSTI:		
	interface (MST	AG and REPAG only)	read, write		
	ethernet-service	es (PVSTAG and PVRSTAG only) read, write		
Task ID	Task ID		Operations		
		is used when configuring Access I in the BPDUs sent from this inte	Gateway to set the bridge priority that is advertised for th rface.		
Usage Guidelines			associated with a task group that includes appropriate tas u from using a command, contact your AAA administrate		
	Release 4.0.0 This command was supported in the PVSTAG and PVRSTAG configuration mode.				
	Release 3.7.1	This command was introduced.			
Command History	Release	Modification			
Command Modes	MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration, PVRSTAG VLAN configuration				
Command Default	Default value is 32768. If the startup value is not specified while the standard value is, the startup value defaults to the standard value.				
	startup-priority	P Specifies the startup priority.			
	startup-value	Sets an alternate value to use w timer is running.	hen the interface first comes up, while the preempt delay		
Syntax Description	priority		MSTAG, REPAG and PVRSTAG, the range is between For PVSTAG, the range is between 0 to 65535.		

priority (MSTP)

To set the bridge priority for the current MSTI, use the priority command in MSTI configuration submode.

priority priority

Syntax Description	<i>priority</i> Bridge priority for the current MSTI. Range is 0 to 61440 in multiples of 4096.		
Command Default	priority: 327	768	
Command Modes	MSTI config	guration	
Command History	Release	Modification	
	Release 3.7	.1 This command was introduced.	
Usage Guidelines		ser group assignment is preventing	oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task ID 0	perations	
	interface re w	ead, vrite	
Examples	The following	ng example shows how to set the b	pridge priority to 8192 for the current MSTI:
	RP/0/RSP0/	CPU0:router(config-mstp-inst)	# priority 8192
Related Commands	Command		Description
	debug span	ning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug span page 347	ning-tree mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	instance (N	ISTP), on page 368	Enters the multiple spanning tree instance (MSTI) configuration submode.
	spanning-tr	ree mst, on page 443	Enters the MSTP configuration submode
	show spanr	ning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.

provider-bridge (MSTAG/REPAG)

To place the current instance of the protocol in 802.1ad mode, use the **provider-bridge** command in MSTAG or REPAG interface configuration submode.

provider-bridge

Syntax Description

This command has no keywords or arguments.

I

Command Default	The default	value is F	ALSE.	
Command Modes	MSTAG int	terface cor	nfiguration, REPAG inte	rface configuration
Command History	Release	Modif	ication	-
	Release 3.7	7.1 This c introd	ommand was uced.	-
Usage Guidelines		iser group		roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task ID (Operations		
	interface r	read, write		
Examples			le shows how to use the	provider-bridge command: # provider-bridge
Related Commands	Command			Description
	debug spar 348	nning-tree	mstag packet, on page	Enables MSTAG packet debugging.
	debug spar 355	nning-tree	repag packet, on page	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface (I	MSTAG/RE	PAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	spanning-t	ree mstag	, on page 444	Enters the MST Access Gateway configuration submode.
			, on page 444 , on page 448	
	spanning-t	ree repag,		Enters the MST Access Gateway configuration submode. Enters the Resilient Ethernet Protocol Access Gateway (REPAG)

provider-bridge (MSTP)

To place the current instance of the protocol in 802.1ad mode, use the **provider-bridge** command in MSTP configuration submode.

provider-bridge

Syntax Description	This comman	d has no keywords or arguments	3.
Command Default	The default v	alue is FALSE.	
Command Modes	MSTP config	uration	
Command History	Release	Modification	
	Release 3.7.1	This command was introduced.	
Usage Guidelines		er group assignment is preventin	roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task ID Op	erations	
	interface rea wr		
Examples	The following	g example shows how to use the	provider-bridge command:
	RP/0/RSP0/C	PU0:router(config-mstp)# pr	ovider-bridge
Related Commands	Command		Description
	spanning-tre	e mst, on page 443	Enters the MSTP configuration submode

revision (MSTAG/REPAG)

To set the revision level in the BPDUs sent from this interface, use the **revision** command in MSTAG or REPAG interface configuration submode.

	revision revis	sion-number	
Syntax Description	revision-numl	ber Revision level of the MSTI	Pregion. Range is 0 to 65535.
Command Default	revision-numb	<i>er:</i> 0	
Command Modes	MSTAG interf	face configuration, REPAG inte	erface configuration
Command History	Release	Modification	_
	Release 3.7.1	This command was introduced.	-

To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. Task ID Task ID Operations interface read, write **Examples** The following example shows how to set the revision level of the MSTP region to 1: RP/0/RSP0/CPU0:router(config-mstag-if)# revision 1 **Related Commands** Command Description Enables MSTAG packet debugging. debug spanning-tree mstag packet, on page 348 Enables Resilient Ethernet Protocol (REP) Access Gateway debug spanning-tree repag packet, on page debugging commands. 355 Enter the MSTAG interface configuration submode, and enables interface (MSTAG/REPAG), on page 371 MSTAG for the specified port. Enters the MST Access Gateway configuration submode. spanning-tree mstag, on page 444 Enters the Resilient Ethernet Protocol Access Gateway (REPAG) spanning-tree repag, on page 448 configuration submode. Displays the values currently used for populating the BPDUs show spanning-tree mstag, on page 426 sent by all ports. Displays the values currently used for populating the BPDUs show spanning-tree repag, on page 438 sent by all ports.

revision (MSTP)

To set the revision level of the MSTP region, use the revision command in MSTP configuration submode.

	revision revision-number
Syntax Description	<i>revision-number</i> Revision level of the MSTP region. Range is 0 to 65535.
Command Default	revision-number: 0
Command Modes	MSTP configuration

Command History	Releas	e	Modification	
	Releas		This command was introduced.	
Usage Guidelines		he user		oup associated with a task group that includes appropriate task you from using a command, contact your AAA administrator
Task ID	Task ID	Operat	ions	
	interface	. `		
		write		
Examples		lowing	-	evision level of the MSTP region to 10:
	RP/0/R:	lowing o	example shows how to set the re 10:router(config-mstp)# rev	ision 10
	RP/0/R	lowing of spo/cpt	-	-
Examples Related Commands	RP/0/R: Comma debug	lowing of spo/cpt and spannin spannin	0:router(config-mstp)# rev	ision 10 Description
	RP/0/R Comma debug debug page 3	lowing of spo/cpt and spannin spannin 47	0:router(config-mstp)# rev g-tree mst packet, on page 345	Description Enables debugging for sent and received MSTP packets. Enables debugging protocol-state changes such as port role

root-cost

To set the root path cost to sent in BPDUs from this interface, use the **root-cost** command in PVSTAG VLAN configuration or PVRSTAG VLAN configuration mode.

root-cost cost [startup-value startup-cost]

Syntax Description	cost	Sets the root path cost for the current port. The cost ranges between 0 to 4294967295.
	startup-value	Specifies an alternate value to use when the interface first comes up, while the preempt delay timer is running.
	startup-cost	Sets the startup cost.

Command Default The default is 0. If a cost is configured but no startup value is configured, the startup value defaults to the configured cost value. If no cost is configured, the startup value defaults to 1.

Command Modes	PVSTAG VI	AN configuration, PVRSTA	G VLAN configuration
Command History	Release	Modification	
	Release 4.0.	0 This command was introduced.	
Usage Guidelines		er group assignment is prever	er group associated with a task group that includes appropriate task nting you from using a command, contact your AAA administrator
Task ID	Task ID	Operations	
	ethernet-serv	ices read, write	
Examples	The followin	g example shows how to set t	he root path cost for the current port:
	RP/0/RSP0/C	PU0:router(config-pvrsta	g-if-vlan)# root-cost 1000000
Related Commands	Command		Description
	debug spani page 352	ning-tree pvrstag packet, on	Enables packet debugging for sent and received PVRSTAG packets.
	debug spani page 354	ning-tree pvstag packet, on	Enables packet debugging for sent and received PVSTAG packets.
	interface (P\		Entere DVCT or DVDCT Access Cotoway Interface configuration
		/STAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
		ing-tree pvrstag, on page 3/5	submode and enables either PVSTAG or PVRSTAG for the specified port.
	show spann		submode and enables either PVSTAG or PVRSTAG for the specified port. Displays the values currently used for populating the BPDUs sent by all ports.
	show spann show spann	ing-tree pvrstag, on page 435	submode and enables either PVSTAG or PVRSTAG for the specified port. Displays the values currently used for populating the BPDUs sent by all ports. Displays the values currently used for populating the BPDUs sent
	show spann show spann spanning-tre	ing-tree pvrstag, on page 435 ing-tree pvstag, on page 436	submode and enables either PVSTAG or PVRSTAG for the specified port. Displays the values currently used for populating the BPDUs sent by all ports. Displays the values currently used for populating the BPDUs sent by all ports. Enters the Per VLAN Rapid Spanning Tree Access Gateway

root-id

To set the identifier of the root bridge for BPDUs sent from a port and an optional startup-value, use the **root-id** command in the MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration and PVRSTAG VLAN configuration modes.

root-id *id* [**startup-value** *startup-id*]

Syntax Description	id	Sets the root bridge ID (MAC add	ress) to set	in the BPDUs.	
	startup-value	Specifies an alternate value to use v timer is running.	when the int	erface first comes up, while the preempt delay	
	startup-id	Sets the startup root ID.			
Command Default	the startup valu		r MSTAG a	te is not specified while the standard value is, nd REPAG, the default is the bridge ID. For	
Command Modes	MSTAG instant VLAN configu		configuratio	n, PVSTAG VLAN configuration, PVRSTAG	
Command History	Release	Modification			
	Release 3.7.1 This command was introduced.				
		This command was supported in th modes.	e PVSTAG	VLAN and PVRSTAG VLAN configuration	
Usage Guidelines		· · · ·		with a task group that includes appropriate task g a command, contact your AAA administrator	
Task ID	Task ID		Operations		
	ethernet-servic	es (PVSTAG and PVRSTAG only)	read, write		
	interface (MST	TAG and REPAG only)	read, write		
Examples	The following e	example shows how to set the ident	ifier of the 1	root bridge for BPDUs:	

I

RP/0/RSP0/CPU0:router(config-pvstag-if-vlan)#root-id 0000.0000.0000 startup-value
0000.0001

Command	Description
debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
debug spanning-tree pvrstag packet, on page 352	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-tree pvstag packet, on page 354	Enables packet debugging for sent and received PVSTAG packets.
debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
interface (MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
interface (PVSTAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
instance (MSTAG/REPAG), on page 367	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.
	debug spanning-tree mstag packet, on page 348debug spanning-tree pvstag packet, on page 352debug spanning-tree pvstag packet, on page 354debug spanning-tree repag packet, on page 355interface (MSTAG/REPAG), on page 371interface (PVSTAG/PVRSTAG), on page 375instance (MSTAG/REPAG), on page 367spanning-tree mstag, on page 444spanning-tree pvstag, on page 444spanning-tree pvstag, on page 444spanning-tree pvstag, on page 444spanning-tree pvstag, on page 445show spanning-tree mstag, on page 448show spanning-tree mstag, on page 448show spanning-tree pvstag, on page 435show spanning-tree pvstag, on page 436show spanning-tree pvstag, on page 438

root-priority

To set the root bridge priority sent in BPDUs for this interface for this MSTI or VLAN, and to set an optional startup value, use the **root-priority** command in the MSTAG instance configuration, REPAG instance configuration, PVSTAG VLAN configuration and PVRSTAG VLAN configuration modes.

root-priority priority [startup-value startup-priority]

Syntax Description	priority		in the BPDUs. For MSTAG, REPAG and PVRSTAG, n multiples of 4096. For PVSTAG, the range is between
	startup-value	Specifies an alternate value to use delay timer is running.	e when the interface first comes up, while the preempt
	startup-priority	Sets the startup root priority.	
Command Default	Default value is defaults to the s		pecified while the standard value is, the startup value
	For MSTAG an	d REPAG, the default is 32768. For	PVSTAG and PVRSTAG, the default is 0.
Command Modes	MSTAG instand VLAN configur		onfiguration, PVSTAG VLAN configuration, PVRSTAG
Command History	Release	Modification	
	Release 3.7.1	This command was introduced.	
		This command was supported in the modes.	e PVSTAG VLAN and PVRSTAG VLAN configuration
Usage Guidelines			associated with a task group that includes appropriate task from using a command, contact your AAA administrator
Task ID	Task ID		Operations
	ethernet-service	es (PVSTAG and PVRSTAG only)	read, write
	interface (MST	AG and REPAG only)	read, write
Examples	The following e	example shows how to set the root b	oridge priority for the current MSTI:

RP/0/RSP0/CPU0:router(config-pvstag-if-vlan)# root-priority 4096 startup-value 8192

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	debug spanning-tree pvrstag packet, on page 352	Enables packet debugging for sent and received PVRSTAG packets.
	debug spanning-tree pvstag packet, on page 354	Enables packet debugging for sent and received PVSTAG packets.
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface (MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	interface (PVSTAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
	instance (MSTAG/REPAG), on page 367	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
	spanning-tree pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
	spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.
	vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

show ethernet mvrp mad

To display the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port, for each active attribute value (VID), use the **show ethernet mvrp mad** command in EXEC mode.

show ethernet mvrp mad [brief] [interface interface-name] [vlan vlan-id]

Syntax Description	brief	(Optional) Displ	lays a brief view.
	interface	(Optional) Displ	ays the MVRP state for the given subinterface or base interface name.
	interface-nam		lays the interface name.
	vlan vlan-id		ays information for a particular VLAN. The range is between 0 to 4094.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 3.7.2	This command wa introduced.	as
Usage Guidelines	To use this cor	introduced.	e in a user group associated with a task group that includes appropriate task is preventing you from using a command, contact your AAA administrator
Usage Guidelines Task ID	To use this cor IDs. If the user	introduced.	e in a user group associated with a task group that includes appropriate task
	To use this cor IDs. If the user for assistance.	introduced. nmand, you must b r group assignment Operations	e in a user group associated with a task group that includes appropriate task
	To use this cor IDs. If the user for assistance. Task ID ethernet-service	introduced. nmand, you must b r group assignment Operations es read	e in a user group associated with a task group that includes appropriate task
Task ID	To use this cor IDs. If the user for assistance. Task ID ethernet-service The following RP/0/RSP0/CP GigabitEther Participan	introduced. mmand, you must b r group assignment Operations es read sample output is fr U0:router# show net0/1/0/1 t Type: Full; Po	e in a user group associated with a task group that includes appropriate task is preventing you from using a command, contact your AAA administrator rom the show ethernet mvrp mad command: ethernet mvrp mad interface GigabitEthernet 0/1/0/1 pint-to-Point: Yes
Task ID	To use this cor IDs. If the user for assistance. Task ID ethemet-service The following RP/0/RSP0/CP GigabitEther Participan Admin Cont LeaveAll P Leave in 2	introduced. nmand, you must b r group assignment Operations es read sample output is fr U0:router# show net0/1/0/1 t Type: Full; Por rol: Applicant N assive (next in 5.70s; Join not	e in a user group associated with a task group that includes appropriate task is preventing you from using a command, contact your AAA administrator rom the show ethernet mvrp mad command: ethernet mvrp mad interface GigabitEthernet 0/1/0/1 Sint-to-Point: Yes lormal; Registrar Normal 5.92s); periodic disabled

I

	1 Very Anxious Observer Leaving 283 Quiet Passive Empty		
Related Commands	Command	Description	
	debug ethernet mvrp packets, on page 343	Enables debugging of sent and received MVRP packets.	
	debug ethernet mvrp protocol, on page 344	Enables MVRP protocol debugging on a specific interface, location or vlan.	
	mvrp static, on page 387	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.	
	show ethernet mvrp statistics, on page 410	Displays packet statistics per port.	
	show ethernet mvrp status, on page 411	Displays a summary of the VIDs that are declared or registered.	

show ethernet mvrp statistics

To display packet statistics per port, use the show ethernet mvrp statistics command in EXEC mode.

show ethernet mvrp statistics [interface type interface-path-id]

Syntax Description	interface (Optional) Displays the MVRP state for the given subinterface or base interface name.						
	<i>type</i> (Optional) Interface type. For more information, use the question mark (?) online he function.						
	interface-path-id (Optional) Physical interface or virtual interface.						
		Note	Use the show interfaces command to see a list of all interfaces currently configured on the router.				
		For more help func	information about the syntax for the router, use the question mark (?) online tion.				
Command Default	None						
Command Modes	EXEC						
Command History	Release M	lodification					
	Release 3.7.2 Thin	his commai troduced.	nd was				
Usage Guidelines			nust be in a user group associated with a task group that includes appropriate task ment is preventing you from using a command, contact your AAA administrator				

Task ID	Task ID	Operations						
Examples	ethernet-services read							
	The following sample output is from the show ethernet mvrp statistics command:							
	RP/0/RSP0/CP GigabitEthern MVRPDUS TX MVRPDUS RX Dropped TX Dropped RX Invalid RX	net0/1/0/1 : 1245 : 7 : 0 : 42	mvrp statistics interface GigabitEthernet 0/1/0/1					
Related Commands	Command		Description					
	debug etherne	et mvrp packets, on page 343	Enables debugging of sent and received MVRP packets.					
	debug etherne	et mvrp protocol, on page 344	Enables MVRP protocol debugging on a specific interface, location or vlan.					
	mvrp static, or	n page 387	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.					
	show etherne	t mvrp mad, on page 409	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.					
	show etherne	t mvrp status, on page 411	Displays a summary of the VIDs that are declared or registered.					

show ethernet mvrp status

To display a summary of the VIDs that are declared or registered, and to learn the origin of these declarations, use the show ethernet mvrp status command in EXEC mode.

Syntax Description	interface	(Optional) Displays the MVRP state for the given subinterface or base interface name.					
	type	(Optional) Interface type. For more information, use the question mark (?) online help function.					
	interface-path-id	ce-path-id (Optional) Physical interface or virtual interface.					
		Note	Use the show interfaces command to see a list of all interfaces currently configured on the router.				
		For more information about the syntax for the router, use the question mark (?) online help function.					
Command Default	None						

show ethernet mvrp status [interface type interface-path-id]

Command Default

Command Modes	EXEC					
Command History	Release	Modification	1	_		
	Release 3.7.	2 This commandation introduced.	nd was	_		
Usage Guidelines		er group assign		group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator		
Task ID	Task ID	Operations				
	ethernet-serv	ices read				
Examples	The following sample output is from the show ethernet mvrp status command:					
	GigabitEthe Staticall	ernet0/1/0/1 y declared: ly declared:	1-512,768,980	mvrp status interface GigabitEthernet 0/1/0/1 -1034		
Related Commands	Command			Description		
	debug ether	net mvrp packe	ets, on page 343	Enables debugging of sent and received MVRP packets.		
	debug ether	net mvrp protoc	col, on page 344	Enables MVRP protocol debugging on a specific interface, location or vlan.		
	mvrp static, on page 387			Enables Multiple VLAN Registration Protocol (MVRP) in static mode.		
	show etherr	iet mvrp mad, o	n page 409	Displays the current state of the Multiple Registration Protocol (MRP) Attribute Declaration (MAD) component on a port.		
	show ethernet mvrp statistics, on page 4		cs, on page 410	Displays packet statistics per port.		

show I2vpn mstp port

To display the internal MSTI number and number of ports for each VLAN, use the **show l2vpn mstp port** command in EXEC mode.

Syntax Description	interface	(Optional) Displays the MSTP state for the given interface.
	type	Interface type. For more information, use the question mark (?) online help function.

show l2vpn mstp port [interface type interface-path-id] [msti value]

	interface-path	-id Physica	al interface or virtu	al interface.	
		Note	Use the show in configured on the	terfaces command to see a list of all interfaces currently e router.	
		For more information about the syntax for the router, use the question mark (?) help function.			
	msti value	(Option from 0	· · ·	ter for Multiple Spanning Tree Instance (MSTI). The range is	
Command Default	None				
Command Modes	EXEC				
Command History	Release	Modificati	on	-	
	Release 3.7.1	This comm introduced		-	
Usage Guidelines				roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator	
Task ID	Task Operat ID	ions			
	l2vpn read				
Examples	The following	sample out	put is from the sho y	w l2vpn mstp port command:	
	RP/0/RSP0/CP	U0:router#	show 12vpn mstr	<pre>p port interface gigabitethernet 0/1/0/0 msti 5</pre>	
Related Commands	Command			Description	
	spanning-tree	mst, on pag	je 443 - E	nters the MSTP configuration submode	
	spanning-tree	mstag, on p	bage 444 E	nters the MST Access Gateway configuration submode.	
	spanning-tree	pvrstag, on	1 0	nters the Per VLAN Rapid Spanning Tree Access Gateway PVRSTAG) configuration submode.	
	spanning-tree	pvstag, on		nters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.	
	spanning-tree	mst, on pag	ge 443 E	nters the MSTP configuration submode	
	spanning-tree	mstag, on p	bage 444 E	Enters the MST Access Gateway configuration submode.	
	show l2vpn m	stp vlan, on		Displays the Multiple Spanning Tree Protocol (MSTP) state for he virtual local area network (VLAN) on a given interface.	

show l2vpn mstp vlan

To display the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface, use the **show l2vpn mstp vlan** command in EXEC mode.

show l2vpn mstp vlan [interface type interface-path-id] [msti value] [vlan-id value]

Syntax Description	interface	(Optional) Displays the MSTP state for the given subinterface or base interface name.			
	type	(Optional) Interface type. For more information, use the question mark (?) online help function.			
	interface-path-id	(Optional) Physical interface or virtual interface.			
		Note Use the show interfaces command to see a list of all interfaces currently configured on the router.			
	For more information about the syntax for the router, use the question mark help function.				
	msti value(Optional) Displays the filter for Multiple Spanning Tree Instance (MSTI). The range is from 0 to 100.				
	vlan-id value	(Optional) Displays the filter for the VLAN ID. The range is from 0 to 4294967295.			
Command Default	None				
Command Modes	EXEC				
Command History	Release Mo	odification			
	Release 3.7.2 Th int	troduced.			
Usage Guidelines		and, you must be in a user group associated with a task group that includes appropriate task oup assignment is preventing you from using a command, contact your AAA administrator			
Task ID	Task Operations ID	;			
	l2vpn read	-			
Examples	The following san	- nple output is from the show l2vpn mstp vlan command:			

RP/0/RSP0/CPU0:router# show l2vpn mstp vlan interface gigabitethernet 0/1/0/0 msti 5 vlan-id 5

Related Comma	nds
----------------------	-----

Command	Description
spanning-tree mst, on page 443	Enters the MSTP configuration submode
spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
spanning-tree pvrstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.
spanning-tree pvstag, on page 447	Enters the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode.
spanning-tree mst, on page 443	Enters the MSTP configuration submode
spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.
show l2vpn mstp port, on page 412	Displays the internal MSTI number and number of ports for each VLAN.

show spanning-tree mst

To display the multiple spanning tree protocol status information, use the **show spanning-tree mst** command in EXEC mode.

show spanning-tree mst protocol instance identifier [instance instance-id] [{blocked-ports|brief}]

Syntax Description	protocol insta	ance identifier	String of a maximum of 25 ch	aracters that identifies the protocol instance.
	instance instance-id brief		Forward interface in rack/slo	t/instance/port format.
			Displays a summary of MST information only.	
	blocked-port	ts	Displays MST information for	or blocked ports only.
Command Default	None			
Command Modes	EXEC			
Command History	Release	Modification	1	-
	Release 3.7.1	This comma	nd was introduced.	-
	Release 3.9.1	The topolog	y-change keyword was added.	-
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate IDs. If the user group assignment is preventing you from using a command, contact your AAA administr for assistance.			

I

Task ID	Task Opera ID	ations						
	interface read							
Examples	-	example shows f the spanning	-		show spannin	g-tree m	st command, which pr	oduces
		PUO:router# s Provider Br ?):	-	ng-tre	e mst a inst	ance O		
	VLANS Mapp	ed: 1-100, 5	00-1000, 1	017				
	Root ID	Priority Address This bridge Hello Time	0004.9b78 is the ro	ot	20 sec For	ward De	lay 15 sec	
	Bridge ID	Priority Address Hello Time			y 4096 sys-i 20 sec For			
	Interface Name			Cost		Cost B	-	Prio.Nbr
	GigabitEther	net0/1/2/1	128.65	20000	DSGN FWD	0 4	097 0004.9b78.0800 097 0004.9b78.0800	128.65
	The following example shows the output from the show spanning-tree mst command when the brief and blocked-ports keywords are used:							
	MSTI 0 (CIST VLAN IDs: This is th MSTI 1: VLAN IDS:	1-100, 500-1 ne Root Bridg	000, 1017 e	-			b78.0812	
	 RP/0/RSP0/CF MSTI 0 (CISI	PU0:router# s]):	how spanni:	ng-tre	e mst blocke	d-ports		
	Interface Name			Cost	Role State	Cost B		Port ID Prio.Nbr
							4097 0004.9b78.0	

Related Commands	Command	Description
	debug spanning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug spanning-tree mst protocol-state, on page 347	Enables debugging protocol-state changes such as port role or state changes, topology change notification.

Description
Displays the internal MSTI number and number of ports for each VLAN.
Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
Displays the contents of MSTP BPDUs being sent and received on a particular interface.
Displays the VLAN ID to MSTI mapping table.
Displays information about misconfiguration affecting MSTP.
Displays detailed information on the interface state.
Displays details of the last topology change that occurred for each pair of port and instance.
Enters the MSTP configuration submode

show spanning-tree mst bpdu interface

To display the contents of MSTP BPDUs being sent and received on a particular interface, use the **show spanning-tree mst bpdu interface** command in the EXEC mode.

show spanning-tree mst protocol instance identifier bpdu interface type interface-path-id [direction {receive | transmit}]

Syntax Description	protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.				
	bpdu interface	Displays multiple spanning tree BPDUs.				
	type	Interface type. For more information, use the question mark (?) online help function.				
	interface-path-id	Physical interface or virtual interface.				
		Note Use the show interfaces command to see a list of all interfaces currently configured on the router.				
		For more information about the syntax for the router, use the question mark (?) online help function.				
	direction	Displays per-interface MST BPDUs for a specific direction.				
	receive	Displays only the MST BPDUs received on this interface.				
	transmit	Displays only the MST BPDUs being transmitted for this interface.				

I

Command Default	None						
Command Modes	EXEC						
Command History	Release	Modification					
	Release 3.7.1	This command was introduced.					
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes approp IDs. If the user group assignment is preventing you from using a command, contact your AAA adm for assistance.						
Task ID	Task Opera ID	ations					
	interface read						
Examples		example shows the output from th BPDUs being output and receive	e show spanning-tree mst command, which produces d on a given local interface:				
Note	Several receive	ed packets can be stored in case	of MSTP operating on a shared LAN.				
Note	RP/0/RSP0/CP direction tr MSTI 0 (CIST Root ID : 00 Path Cost :	U0:router# show spanning-tr ansmit): 04.9b78.0800 83 0004.9b78.0800	of MSTP operating on a shared LAN.				
	RP/0/RSP0/CP direction tr MSTI 0 (CIST Root ID : 00 Path Cost : Bridge ID : Port ID : 12 Hello Time :	U0:router# show spanning-tr ansmit): 04.9b78.0800 83 0004.9b78.0800					
	RP/0/RSP0/CP direction tr MSTI 0 (CIST Root ID : 00 Path Cost : Bridge ID : Port ID : 12 Hello Time : 	U0:router# show spanning-tr ansmit): 04.9b78.0800 83 0004.9b78.0800	ee mst a bpdu interface GigabitEthernet0/1/2/2				
	RP/0/RSP0/CP direction tr MSTI 0 (CIST Root ID : 00 Path Cost : Bridge ID : Port ID : 12 Hello Time : Command debug spannin	U0:router# show spanning-tr ansmit): 04.9b78.0800 83 0004.9b78.0800 2	ee mst a bpdu interface GigabitEthernet0/1/2/2 Description Enables debugging for sent and received MSTP packets.				
	RP/0/RSP0/CP direction tr MSTI 0 (CIST Root ID : 00 Path Cost : Bridge ID : Port ID : 12 Hello Time : Command debug spannin page 347	U0:router# show spanning-tr ansmit): 04.9b78.0800 83 0004.9b78.0800 2 ng-tree mst packet, on page 345	ee mst a bpdu interface GigabitEthernet0/1/2/2 Description Enables debugging for sent and received MSTP packets. Enables debugging protocol-state changes such as port role				
	RP/0/RSP0/CP direction tr MSTI 0 (CIST Root ID : 00 Path Cost : Bridge ID : Port ID : 12 Hello Time : Command debug spannin page 347 show l2vpn m	U0:router# show spanning-tr ansmit): 04.9b78.0800 83 0004.9b78.0800 2 ng-tree mst packet, on page 345 ng-tree mst protocol-state, on	ee mst a bpdu interface GigabitEthernet0/1/2/2 Description Enables debugging for sent and received MSTP packets. Enables debugging protocol-state changes such as port role or state changes, topology change notification. Displays the internal MSTI number and number of ports for each VLAN. Displays the Multiple Spanning Tree Protocol (MSTP) state				
Note Related Commands	RP/0/RSP0/CP direction tr MSTI 0 (CIST Root ID : 00 Path Cost : Bridge ID : Port ID : 12 Hello Time : Command debug spannin page 347 show l2vpn m	U0:router# show spanning-tr ansmit): 04.9b78.0800 83 0004.9b78.0800 2 ng-tree mst packet, on page 345 ng-tree mst protocol-state, on stp port, on page 412	ee mst a bpdu interface GigabitEthernet0/1/2/2 Description Enables debugging for sent and received MSTP packets. Enables debugging protocol-state changes such as port role or state changes, topology change notification. Displays the internal MSTI number and number of ports for each VLAN.				

Command	Description
show spanning-tree mst errors, on page 420	Displays information about misconfiguration affecting MSTP.
show spanning-tree mst interface, on page 421	Displays detailed information on the interface state.
show spanning-tree mst topology-change flushes, on page 424	Displays details of the last topology change that occurred for each pair of port and instance.
spanning-tree mst, on page 443	Enters the MSTP configuration submode

show spanning-tree mst configuration

To display the VLAN ID to MSTI mapping table, use the **show spanning-tree mst configuration** command in the EXEC mode.

show spanning-tree mst protocol instance identifier configuration

Syntax Description	protocol instance identifier String of a maximum of 25 characters that identifies the protocol instance.					
	configuration		Displays a summary of MST related configuration.			
Command Default	None					
Command Modes	EXEC					
Command History	Release	Modification	1			
	Release 3.7.1	This commai introduced.	nd was			
Usage Guidelines		mand, you m	nust be in a user group associated with a task group that includes appropriate tas			
	IDs. If the user for assistance.		ment is preventing you from using a command, contact your AAA administrato			
Task ID		group assign				
Task ID	for assistance. Task Operat	group assign				
	for assistance. Task Operat ID interface read	group assign ions xample show	ment is preventing you from using a command, contact your AAA administrato			
Task ID Examples	for assistance. Task Operat ID interface read The following e the VLAN ID t RP/0/RSP0/CPU Name Revision	stand a standard a sta	ment is preventing you from using a command, contact your AAA administrato			

1-9,11-19,21-29,31-39,41-4094 10,20,30,40

1 -----

Related Commands	Command	Description
	debug spanning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug spanning-tree mst protocol-state, on page 347	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	show l2vpn mstp port, on page 412	Displays the internal MSTI number and number of ports for each VLAN.
	show l2vpn mstp vlan, on page 414	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
	show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.
	show spanning-tree mst bpdu interface, on page 417	Displays the contents of MSTP BPDUs being sent and received on a particular interface.
	show spanning-tree mst errors, on page 420	Displays information about misconfiguration affecting MSTP.
	show spanning-tree mst interface, on page 421	Displays detailed information on the interface state.
	show spanning-tree mst topology-change flushes, on page 424	Displays details of the last topology change that occurred for each pair of port and instance.
	spanning-tree mst, on page 443	Enters the MSTP configuration submode

show spanning-tree mst errors

To display information about misconfiguration affecting MSTP, use the show spanning-tree mst errors in the EXEC mode.

show spanning-tree mst protocol instance identifier errors

Syntax Description	protocol insta	ince identifier	String of a maximum of 25 characters that identifies the protocol instance.
	errors		Displays configuration errors for MST.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 3.7.1	This commanintroduced.	ıd was

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate t IDs. If the user group assignment is preventing you from using a command, contact your AAA administration for assistance.						
Task ID	Task ID	Operations					
	interface	read					
Examples	The following example shows the output from the show spanning-tree mst command, which produces information about interfaces that are configured for MSTP but where MSTP is not operational. Primarily this shows information about interfaces which do not exist:						
	RP/0/RS Interfa		ater# show spanning-ta Error	ree mst a errors			
	Gigabit	tEthernet1/2	2/3/4 Interface does	not exist.			
Related Commands	Comma	and		Description			
	debug	spanning-tree	e mst packet, on page 345	Enables debugging for sent and received MSTP packets.			
	debug page 34		e mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.			
	show 12	2vpn mstp poi	t, on page 412	Displays the internal MSTI number and number of ports for each VLAN.			
	show 12	2vpn mstp vla	n, on page 414	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.			
	show s	panning-tree	mst, on page 415	Displays the multiple spanning tree protocol status information.			
	show s page 4	• •	mst bpdu interface, on	Displays the contents of MSTP BPDUs being sent and received on a particular interface.			
	show s 419	panning-tree	mst configuration, on page	Displays the VLAN ID to MSTI mapping table.			
	show s	panning-tree	mst interface, on page 421	Displays detailed information on the interface state.			
		panning-tree , on page 424	mst topology-change	Displays details of the last topology change that occurred for each pair of port and instance.			
	spannii	ng-tree mst, c	on page 443	Enters the MSTP configuration submode			

show spanning-tree mst interface

To display detailed information on the interface state, use the **show spanning-tree mst interface** command in EXEC mode.

	protocori	instance identifi	er String c	f a maximum of 25 characters that identifies the protocol instance.			
	interface	e type		Interface type. For more information, use the question mark (?) online help function.			
	interface-path-id		Physica	l interface or virtual interface.			
			Note	Use the show interfaces command to see a list of all interfaces currently configured on the router.			
			For more information about the syntax for the router, use the question mark (?) online help function.				
	instance	id	Forward	l interface in rack/slot/instance/port format.			
Command Default	None						
Command Modes	EXEC						
Command History	Release	Modificat	on				
	Release 3	5.7.1 This comr introduced					
Usage Guidelines		user group assi		a user group associated with a task group that includes appropriate task preventing you from using a command, contact your AAA administrator			
Task ID	Task (ID	Operations					
Task ID		·					
	ID interface 1 The follow	read		but from the show spanning-tree mst command, which produces interface state than the standard command as described above:			
	ID interface 1 The follow more deta RP/0/RSP0 3 GigabitE Cost: 200	read ving example sho iled information 0/CPU0:router thernet0/1/2/2 000 e: point-to-po me 1 : no rd: no	n regarding # show spa				
Task ID Examples	ID interface in The follow more deta RP/0/RSP4 3 GigabitE Cost: 200 link-type hello-tin Portfast BPDU Gua: Guard roo Guard top	read ving example sho iled information 0/CPU0:router thernet0/1/2/2 000 e: point-to-po me 1 : no rd: no	show spa show spa l bint no	interface state than the standard command as described above:			

show spanning-tree mst protocol instance identifier interface type interface-path-id [instance id]

```
Boundary : internal
Designated forwarding
Vlans mapped to MST 3: 1-2,4-2999,4000-4094
Port info port id 128.193 cost 200000
Designated root address 0050.3e66.d000 priority 8193 cost 20004
Designated bridge address 0002.172c.f400 priority 49152 port id 128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Transitions to reach this state: 12
```

The output includes interface information about the interface which applies to all MSTIS:

- Cost
- link-type
- hello-time
- portfast (including whether BPDU guard is enabled)
- guard root
- guard topology change
- BPDUs sent, received.

It also includes information specific to each MSTI:

- · Port ID, priority, cost
- BPDU information from root (bridge ID, cost, and priority)
- BPDU information being sent on this port (Bridge ID, cost, priority)
- State transitions to reach this state.
- Topology changes to reach this state.

Flush containment status for this MSTI.

Related Commands	Command	Description
	debug spanning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug spanning-tree mst protocol-state, on page 347	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	show l2vpn mstp port, on page 412	Displays the internal MSTI number and number of ports for each VLAN.
	show l2vpn mstp vlan, on page 414	Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.
	show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.
	show spanning-tree mst bpdu interface, on page 417	Displays the contents of MSTP BPDUs being sent and received on a particular interface.
	show spanning-tree mst configuration, on page 419	Displays the VLAN ID to MSTI mapping table.
	show spanning-tree mst errors, on page 420	Displays information about misconfiguration affecting MSTP.
	show spanning-tree mst topology-change flushes, on page 424	Displays details of the last topology change that occurred for each pair of port and instance.
	spanning-tree mst, on page 443	Enters the MSTP configuration submode

show spanning-tree mst topology-change flushes

To display details of the last topology change that occurred for each pair of port and instance, as well as a count of the number of topology changes at each port, use the **show spanning-tree mst topology-change flushes** command in the EXEC mode.

show spanning-tree mst protocol instance identifier topology-change flushes [instance *id*] [{interface type interface-path-id | latest}]

Syntax Description	protocol insta	unce identifier	String of a maximum of 25 characters that identifies the protocol instance.				
	topology-cha	inge	Displays topology change information.				
	flushes		Displays	latest topology change flushes for each interface.			
	instance id		Instance	for which information needs to be displayed.			
	interface type	е	Interface function.	type. For more information, use the question mark (?) online help			
	interface-path	h-id	Physical	interface or virtual interface.			
			Note	Use the show interfaces command to see a list of all interfaces currently configured on the router.			
			For more information about the syntax for the router, use the question mark (?) online help function.				
	latest	Displays the most recent topology change for each instance.					
Command Default	None						
Command Modes	EXEC						
Command History	Release Modification		1				
	Release 3.7.1 This command was introduced.		nd was				
Usage Guidelines		r group assign		user group associated with a task group that includes appropriate task eventing you from using a command, contact your AAA administrator			
Note				recent topology change for each instance. The output also displays takes place when the flush containment is active on an MSTI for a port.			

Task ID	Task ID	Operatio	ons					
	interface	e read						
Examples	The following example shows the output from the show spanning-tree mst command, which displays details on the MSTIs :							
	RP/0/RS MSTI 1:		:router# show span	ning-tr	ee mst M topology-change	flushes instance\$		
	Interfa	ace	Last TC	Rea	son	Count		
	 Te0/0/0 # #	0/1	04:16:05 Mar 16 20	 10 Rol	e change: DSGN to	10		
		SP0/CPU((CIST):	-	ning-tr	ee mst M topology-change	flushes instance\$		
	Interfa	ace	Last TC		son	Count		
	Te0/0/(# #	0/1			e change: DSGN to	10		
Related Commands	Comma	and			Description			
	debug	spanning	j-tree mst packet, on p	age 345	Enables debugging for sent a	and received MSTP packets.		
	debug page 34		I-tree mst protocol-sta	te, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.			
	show 12	2vpn mst	p port, on page 412		Displays the internal MSTI n each VLAN.	umber and number of ports for		
	show 12	2vpn mst	p vlan, on page 414		Displays the Multiple Spanning Tree Protocol (MSTP) state for the virtual local area network (VLAN) on a given interface.			
	show s	panning-	tree mst, on page 415		Displays the multiple spanning	g tree protocol status information.		
	show s page 4		tree mst bpdu interfac	e, on	Displays the contents of MST on a particular interface.	P BPDUs being sent and received		
	show s 419	panning-	tree mst configuration,	on page	Displays the VLAN ID to MS	TI mapping table.		
	show s	panning	tree mst errors, on pa	ge 420	Displays information about misconfiguration affecting MSTF			
	show s	panning-	tree mst interface, on p	bage 421	Displays detailed information	n on the interface state.		
	spannii	ng-tree n	nst, on page 443		Enters the MSTP configurati	on submode		
	-							

show spanning-tree mstag

To display the values currently used for populating the BPDUs sent by all ports (with the specified feature enabled), use the **show spanning-tree mstag** in the EXEC mode.

show spanning-tree mstag protocol instance identifier

Syntax Description						
Syntax Bescription	protocol instance identifier String (a maximum of 25 characters) that identifies the protocol instance.					
Command Default	None					
Command Modes	EXEC					
Command History	Release Modification					
	Release 3.7.1 This command was introduced.					
	Release 4.1.0 The show output of this command was modified to include information on the MSTAG Edge Mode feature.					
	Release 6.2.2 The show output of this command was modified to include information on core connectivity status. If core connectivity is available, the device displays that the standard BPDU is sent, else the it displays that the start-up BPDU is sent.					
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.					
Task ID	Task ID Operations					
	interface read					
Examples						
	This example shows the output from the show spanning-tree mstag command:					

L

Port Priority: 128 Cost: 0 Root Bridge: 6161.6161.6161 Root Priority: 32768 Topology Changes: 123 MSTI 2 VLAN IDs: 10-31 Role: Designated Bridge Priority: 32768 Port Priority: 128 Cost: 0 Root Bridge: 6161.6161.6161 Root Priority: 32768 Topology Changes: 123 MSTI 10 VLAN IDs: 40 Role: Root (Edge mode) Bridge Priority: 32768 Port Priority: 128 200000000 Cost: 6161.6161.6161 Root Bridge: Root Priority: 61440 Topology Changes: 0 RP/0/RSP0/CPU0:router# show spanning-tree mstag foo GigabitEthernet0/0/0/0 Pre-empt delay is disabled. Core connectivity tracking is enabled Sending startup BPDU as core connectivity is unavailable Name: 029d:af84:4100 Revision: 0 Max Age: 20 Provider Bridge: no Bridge ID: 029d.af84.4100 Port ID: 1 200000000 2 External Cost: Hello Time: Active: no Packets sent: 184 Auto-configure edge: no MSTI 0 (CIST): VLAN IDs: 1-4094 Role: Designated Bridge Priority: 32768 Port Priority: 128 200000000 Cost: 029d.af84.4100 Root Bridge: Root Priority: 32768 Topology Changes: 0

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	show spanning-tree mstag bpdu interface, on page 428	Displays the content of the BPDUs being sent from this interface.
	show spanning-tree mstag topology-change flushes, on page 429	Displays details of the last topology change that occurred for each pair of port and instance.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.

show spanning-tree mstag bpdu interface

To view the content of the BPDUs being sent from this interface, use the **show spanning-tree mstag bpdu interface** command in the EXEC mode.

show spanning-tree mstag protocol instance identifier bpdu interface type interface-path-id

Syntax Description	<i>protocol instance identifier</i> String of a maximum of 25 characters that identifies the protocol instance.					
	bpdu interface	Displays multiple spanning tree BPDUs. Interface type. For more information, use the question mark (?) online help function.				
	type					
	interface-path-id	Physical interface or virtual interface.				
		Note Use the show interfaces command to see a list of all interfaces currently configured on the router.				
		For more information about the syntax for the router, use the question mark (?) online help function.				
Command Default	None					
Command Modes	EXEC					
Command History	Release Modificati	on				
	Release 3.7.1 This commintroduced					
Usage Guidelines		n must be in a user group associated with a task group that includes appropriate task gnment is preventing you from using a command, contact your AAA administrator				
Task ID	Task Operations ID					
	interface read					
Examples	The following example shows the output from the show spanning-tree mstag bpdu interface command:					
	RP/0/RSP0/CPU0:router Transmitted: MSTI 0 (CIST): ProtocolIdentifier: 0 ProtocolVersionIdentif BPDUType: 2	#show spanning-tree mstag foo bpdu interface GigabitEthernet 0/0/0/0 fier: 3				

```
CISTFlags: Top Change Ack 0
           Agreement
                           1
           Forwarding
                           1
           Learning
                          1
                           3
           Role
           Proposal
                           0
           Topology Change 0
CISTRootIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTExternalPathCost: 0
CISTRegionalRootIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTPortIdentifierPriority: 8
CISTPortIdentifierId: 1
MessageAge: 0
MaxAge: 20
HelloTime: 2
ForwardDelay: 15
Version1Length: 0
Version3Length: 80
FormatSelector: 0
Name: 6969:6969:6969
Revision: 0
MD5Digest: ac36177f 50283cd4 b83821d8 ab26de62
CISTInternalRootPathCost: 0
CISTBridgeIdentifier: priority 8, MSTI 0, address 6969.6969.6969
CISTRemainingHops: 20
 MSTI 1:
                           0
MSTIFlags: Master
          Agreement
                           1
           Forwarding
                           1
                           1
           Learning
           Role
                           3
           Proposal
                           0
           Topology Change 0
MSTIRegionalRootIdentifier: priority 8, MSTI 1, address 6969.6969.6969
MSTIInternalRootPathCost: 0
MSTIBridgePriority: 1
MSTIPortPriority: 8
MSTIRemainingHops: 20
```

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree mstag topology-change flushes, on page 429	Displays details of the last topology change that occurred for each pair of port and instance.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.

show spanning-tree mstag topology-change flushes

To display details of the last topology change that occurred for each pair of port and instance, as well as a count of the number of topology changes at each port, use the **show spanning-tree mstag topology-change flushes** command in the EXEC mode.

Note	The latest filter displays only the most recent topology change for each instance. The output also displays information of the flush operation that takes place when the flush containment is active on an MSTI for a port.					
	-	-	mstag protoc erface-path-id	<pre>ol instance identifier topology-change flushes [instance id] latest}]</pre>		
Syntax Description	protocol in	stance ide	ntifier String o	f a maximum of 25 characters that identifies the protocol instance.		
	topology-c	hange	Displays	s topology change information.		
	flushes		Displays	s latest topology change flushes for each interface.		
	instanceid		Forward	interface in rack/slot/instance/port format.		
	interface a	type	Interface	e type. For more information, use the question mark (?) online help		
	interface-p	ath-id	Physical	interface or virtual interface.		
			Note	Use the show interfaces command to see a list of all interfaces currently configured on the router.		
	latest			For more information about the syntax for the router, use the question mark (?) online help function. Displays the most recent topology change for each instance.		
			Displays			
Command Default	None					
Command Modes	EXEC					
Command History	Release	Modifi	cation			
	Release 3.7	.1 This controduction	ommand was uced.			
Usage Guidelines		ser group		a user group associated with a task group that includes appropriate task reventing you from using a command, contact your AAA administrator		
Task ID	Task Op ID	erations				
	interface rea	ad				
Examples				put from the show spanning-tree mstag topology-change tails on the MSTIs :		

RP/0/RSP0/CPU0:router# show spanning-tree mstag b topology-change flushes

MSTAG Protocol Instance b

Interface	Last TC	Reason	Count
Gi0/0/0/1	18:03:24 2009-07-14	Gi0/0/0/1.10 egress TCN	65535
Gi0/0/0/2	21:05:04 2009-07-15	Gi0/0/0/2.1234567890 ingress TCN	2

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree mstag bpdu interface, on page 428	Displays the content of the BPDUs being sent from this interface.
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.

show spanning-tree mstag tracked

To display the core connectivity tracking data, use the **show spanning-tree mstag tracked** command in the EXEC mode.

show	spanning-tree	mstag	protocol	instance	identifier tracked
------	---------------	-------	----------	----------	---------------------------

Syntax Description	protocol in	stance identifier String (a maxim	im of 25 characters) that identifies the protocol instance.
	tracked	Displays the cor	e connectivity tracking data.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
	Release 6.2.2	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 tas IDs. If the user group assignment is preventing you from using a command, contact your AAA administrate for assistance.		
Task ID	Task ID 0	perations	
	interface re		

Examples This example shows the output from the **show spanning-tree mstag foo tracked** command: RP/0/RSP0/CPU0:router# show spanning-tree mstag foo tracked Core Connectivity Available: True Tracked Items: 1/2 up Interface Name State _____ GigabitEthernet0/0/0/3 Down GigabitEthernet0/0/0/2 Up _____ **Related Commands** Command Description Enables MSTAG packet debugging. debug spanning-tree mstag packet, on page 348 show spanning-tree mstag bpdu interface, on page Displays the content of the BPDUs being sent from this interface. 428 Displays details of the last topology change that occurred show spanning-tree mstag topology-change for each pair of port and instance. flushes, on page 429 Enters the MST Access Gateway configuration submode. spanning-tree mstag, on page 444

show spanning-tree pvrst

To display the Per VLAN Rapid Spanning Tree (PVRST) status information, use the **show spanning-tree pvrst** command in EXEC mode.

show spanning-tree pvrst *protocol instance identifier* [{blocked-ports|bpdu|brief|errors|interface |topology-change|vlan}]

Syntax Description	protocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.	
	blocked-ports	Displays PVRST Bridge Protocol Data Unit (BPDU). Displays PVRST Bridge Protocol Data Unit (BPDU).	
	bpdu		
	brief	Displays PVRST Bridge Protocol Data Unit (BPDU).	
	errors	Display configuration errors for PVRST.	
	interface	Displays PVRST information for every interface.	
	topology-change	Displays topology change information.	

I

	vlan		Displays VLAN information.		
Command Default	None				
Command Modes	EXEC				
Command History	Release	Modification			
	Release 5.1	This command introduced.	was		
Usage Guidelines		ser group assigni	nust be in a user group associated with a task group that includes appropriate task ment is preventing you from using a command, contact your AAA administrator		
Task ID	Task ID	Operations			
	ethernet-ser	vices read			
Examples	This example shows the output from the show spanning-tree pvrst command, which produces an overview of the spanning tree protocol state: RP/0/RSP0/CPU0:router# show spanning-tree pvrst MSTP Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup State: FWD=Forwarding, LRN=Learning, BLK=Blocked				
	VLAN 10: Root ID Pi	ciority 4096			
	This bride	b6.4fe9.7b9e ge is the root sec, Forward	Delay 15 sec		
	Address 80 Max Age 20	Priority 4096 b6.4fe9.7b9e sec, Forward Iold count 6	(priority 4096 sys-id-ext 0) Delay 15 sec		
	Pri.Nbr Co	st Bridge ID P			
	Gi0/5/0/0 128.1 20000 DSGN FWD 4096 8cb6.4fe9.7b9e 128.1 Gi0/5/0/2 128.2 20000 DSGN FWD 4096 8cb6.4fe9.7b9e 128.2				
	VLAN 20:				
	Address c(ciority 8192 62.6bac.a07e 9 sec, Forward	Delay 15 sec		
	Bridge ID	Priority 16384	4 (priority 16384 sys-id-ext 0)		

This example shows the output from the **show spanning-tree pvrst** command when the **brief** and **blocked-ports** keywords are used:

```
RP/0/RSP0/CPU0:router# show spanning-tree pvrst st1 brief
VLAN 1 (native-vlan):
 This is the Root Bridge
VLAN 101:
 Root Port GigabitEthernet0/1/2/2 , Root Bridge ID 0002.9b78.0812
RP/0/RSP0/CPU0:router# show spanning-tree pvrst st1 blocked-ports
VLAN 1 (native-vlan):
Interface
         Port ID
                       Role State Designated
                                                   Port ID
          Pri.Nbr Cost
                              Bridge ID
                                                   Pri.Nbr
Gi0/0/0/0 128.1 20000 ---- BLK 4097 0004.9b78.0800 128.195
```

. . .

This example shows the output for the **show spanning-tree pvrst** command when **interface** keyword is used:

```
RP/0/RSP0/CPU0:router#
show spanning-tree pvrst stl interface GigabitEthernet 0/1/2/1 vlan 10
show spanning-tree pvrst MSTP interface gigabitEthernet 0/5/0/0 vlan 10
Gi0/5/0/0
Configured Cost: 20000
link-type: point-to-point
Configured hello-time: 2
Designated hello-time: 2
Portfast: no
BPDU Guard: no
Guard root: no
VLAN 10:
Edge port: no
designated, forwarding
Port info port id 128.1 cost 20000
Designated root address 8cb6.4fe9.7b9e priority 4096 cost 0
Designated bridge address 8cb6.4fe9.7b9e priority 4096 port id 128.1
Timers: message expires in 0 sec, forward delay 0
BPDUs sent 19433, received 19228
Transitions to reach this state: 2
Topology Changes: 1 total, last at 18:47:29 Jul 1 2013
```

This example shows the output for the **show spanning-tree pvrst** command when **errors** keyword is used:

```
RP/0/RSP0/CPU0:router# show spanning-tree pvrst stl errors
Interface Error
```

Gi/2/3/4 Interface does not exist.

This example shows the output for the **show spanning-tree pvrst** command when **bpdu** keyword is used:

```
RP/0/RSP0/CPU0:router#
show spanning-tree pvrst st1 bpdu interface GigabitEthernet 0/1/2/2 vlan 1 direction receive
Received: (0000.0000.000a)
VLAN 1 (native-VLAN):
   Root ID : 0004.9b78.0800
   Path Cost : 83
   Bridge ID : 0004.9b78.0800
   Port ID : 12
   Hello Time : 2
   ...
```

Related Commands	Command	Description
	debug spanning-tree pvrst, on page 351	Enables debugging protocol-state changes such as port role, state changes, and topology change notification.
	spanning-tree pvrst, on page 445	Enters the Per VLAN Rapid Spanning Tree (PVRST) configuration submode.

show spanning-tree pvrstag

To display the values currently used for populating the BPDUs sent by all ports (with the specified feature enabled), use the **show spanning-tree pvrstag** in the EXEC mode.

show spanning-tree pvrstag protocol instance identifier [interface type interface-path-id]

Syntax Description	protocol instance identifier	String c	String of a maximum of 25 characters that identifies the protocol instance.			
	interface type	Interface type. For more information, use the question mark (?) online help function.				
	interface-path-id	Physical interface or virtual interface.				
		Note	Use the show interfaces command to see a list of all interfaces currently configured on the router.			
			re information about the syntax for the router, use the question mark (?) nelp function.			
Command Default	None					

Command Modes EXEC

Command History	Release	Modificati	ion	-
	Release 4.0	.0 This comn introduced		-
Usage Guidelines		ser group assi		roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator
Task ID	Task Op ID	erations		
	interface rea	ad		
Examples	The followi	ng example sh	nows the output from	n the show spanning-tree pvrstag command:
	GigabitEth VLAN 10 Preemp Sub-in Max Ag Root P Root B Cost: Bridge Port P Port P Port I Hello Active BPDUS	ernet0/0/0/2 t delay is o terface: e: riority: ridge: Priority: ID: riority: D: Time: : sent: gy Changes:	1 disabled. GigabitEthernet0 20 0 00000.0000.0000 0 32768 6161.6161.6161 128 1 2 no 0	ree pvrstag interface GigabitEthernet0/0/0/1 /0/0/1.20 (Up)
Related Commands	Command			Description
	debug span 352	ning-tree pvrs	tag packet, on page	Enables packet debugging for sent and received PVRSTAG packets.
	spanning-ti	ree pvrstag, or	n page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode.

show spanning-tree pvstag

To display the values currently used for populating the BPDUs sent by all ports (with the specified feature enabled), use the **show spanning-tree pvstag** in the EXEC mode.

show spanning-tree pvstag protocol instance identifier [interface type interface-path-id]

Syntax Description protocol instance identifier String of a maximum of 25 characters that identifies the protocol instance.

	interface type	Interface type. For more information, use the question mark (?) online help function.		
	interface-path-id	Physical interface or virtual interface.		
		Note Use the show interfaces command to see a list of all interfaces currently configured on the router.		
		For more information about the syntax for the router, use the question mark (?) online help function.		
Command Default	None			
Command Modes	EXEC			
Command History	Release Modificati	 DN		
	Release 4.0.0 This commintroduced			
Usage Guidelines Task ID		must be in a user group associated with a task group that includes appropriate task gnment is preventing you from using a command, contact your AAA administrator		
	interface read			
Examples	The following example sh	ows the output from the show spanning-tree pvstag command:		
	GigabitEthernet0/0/0/1 VLAN 10 Preempt delay is d			

show spanning-tree repag

To display the values currently used for populating the BPDUs sent by all ports (with the specified feature enabled), use the **show spanning-tree repag** in the EXEC mode.

show spanning-tree repag protocol instance identifier [interface type interface-path-id] [brief]

Syntax Description	protocol instance iden	<i>tifier</i> String of a maximum of 25 characters that identifies the protocol instance.
	interface type	Interface type. For more information, use the question mark (?) online help function.
	interface-path-id	Physical interface or virtual interface.
		Note Use the show interfaces command to see a list of all interfaces currently configured on the router.
		For more information about the syntax for the router, use the question mark (?) online help function.
Command Default	None	
Command Modes	EXEC	
Command History	Release Modifie	cation
	Release 3.7.1 This co introdu	
Usage Guidelines		you must be in a user group associated with a task group that includes appropriate task assignment is preventing you from using a command, contact your AAA administrator
Task ID	Task Operations ID	
	interface read	
Examples	The following example	e shows the output from the show spanning-tree repag command:
	RP/0/RSP0/CPU0:rout GigabitEthernet0/0/ VLAN 10 Preempt delay i Sub-interface: Max Age: Root Priority: Root Bridge: Cost:	

```
Bridge ID: 6161.6161.6161
Port Priority: 128
Port ID: 1
Hello Time: 2
Active: no
BPDUs sent: 0
Topology Changes: 123
VLAN 20
```

Related Commands	Command	Description
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	show spanning-tree repag bpdu interface, on page 439	Displays BPDU information from root (bridge ID, cost, and priority) and the BPDU information being sent on the port.
	show spanning-tree repag topology-change flushes, on page 441	Displays details of the last topology change that occurred for each pair of port and instance.
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.

show spanning-tree repag bpdu interface

To display BPDU information from root (bridge ID, cost, and priority) and the BPDU information being sent on the port (Bridge ID, cost, priority) specific to an MSTI, use the show **spanning-tree repag bpdu interface** command in the EXEC mode.

show spanning-tree repag protocol instance identifier [bpdu interface type interface-path-id]

Syntax Description	nrotocol instance identifier	String of a maximum of 25 characters that identifies the protocol instance.				
oyntax booonption		String of a maximum of 25 characters that identifies the protocol mstance.				
	bpdu interface	Displays multiple spanning tree BPDUs.				
	type	Interface type. For more information, use the question mark (?) online help function.				
	interface-path-id	Physical interface or virtual interface.				
		Note Use the show interfaces command to see a list of all interfaces currently configured on the router.				
		For more information about the syntax for the router, use the question mark (?) online help function.				
Command Default	None					
Command Modes	EXEC					

Command History	Release	Modification				
	Release 3.7.1	This command introduced.	was			
Usage Guidelines		r group assignme	t be in a user group associated with a task group that includes appropriate task ent is preventing you from using a command, contact your AAA administrator			
Task ID	Task Opera ID	ations				
	interface read					
Examples			the output from the show spanning-tree repag command, which s being output and received on a given local interface:			
	RP/0/RSP0/CE Transmitted: MSTI 0 (CI ProtocolIden	ST):	<pre>spanning-tree mstag foo bpdu interface GigabitEthernet 0/0/0/0</pre>			
	ProtocolVers BPDUType: 2	ionIdentifier:				
		op Change Ack greement	1			
		'orwarding	1			
		earning ole	1 3			
		roposal	0			
		opology Change				
	CISTRootIdentifier: priority 8, MSTI 0, address 6969.6969.6969 CISTExternalPathCost: 0					
	CISTExternalPathCost: 0 CISTRegionalRootIdentifier: priority 8, MSTI 0, address 6969.6969.6969					
	CISTPortIdentifierPriority: 8					
	CISTPortIder					
	MessageAge: MaxAge: 20	U				
	HelloTime: 2					
	ForwardDelay					
	VersionlLength: 0 Version3Length: 80					
	Version3Length: 80 FormatSelector: 0					
	Name: 6969:6969:6969					
	Revision: 0					
	MD5Digest: ac36177f 50283cd4 b83821d8 ab26de62 CISTInternalRootPathCost: 0					
		lentifier: pric	ority 8, MSTI 0, address 6969.6969.6969			
	MSTIFlags: M	laster	0			
		greement	1			
		'orwarding earning	1 1			
		ole	3			
		roposal	0			
		opology Change	e 0 : priority 8, MSTI 1, address 6969.6969.6969			
			• priority 0, mort 1, audress 0909.0909.0909			

MSTIInternalRootPathCost: 0 MSTIBridgePriority: 1 MSTIPortPriority: 8 MSTIRemainingHops: 20

Related Commands	Command	Description
	debug spanning-tree repag packet, on page 355	Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	show spanning-tree repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.
	show spanning-tree repag topology-change flushes, on page 441	Displays details of the last topology change that occurred for each pair of port and instance.
	spanning-tree repag, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.

show spanning-tree repag topology-change flushes

To display details of the last topology change that occurred for each pair of port and instance, as well as a count of the number of topology changes at each port, use the **show spanning-tree repag topology-change flushes** command in the EXEC mode.

Ø

Note The latest filter displays only the most recent topology change for each instance. The output also displays information of the flush operation that takes place when the flush containment is active on an MSTI for a port.

show spanning-tree repag protocol instance identifier **topology-change flushes** [instance id] [{interface type interface-path-id | latest}]

Syntax Description	protocol instance identifier	• String of a maximum of 25 characters that identifies the protocol instance.	
	topology-change	Displays topology change information.	
	flushes	Displays latest topology change flushes for each interface.	
	instanceid	Forward interface in rack/slot/instance/port format.	
	interface type	Interface type. For more information, use the question mark (?) online help function.	
	interface-path-id	Physical interface or virtual interface.	
		Note Use the show interfaces command to see a list of all interfaces currently configured on the router.	
		For more information about the syntax for the router, use the question mark (?) online help function.	

	1-4	D' 1 4		in stan a s
	latest	Displays the	e most recent topology change for each	instance.
Command Default	None			
Command Modes	EXEC			
Command History	Release	Modification		
	Release 3.7.1	This command was introduced.		
Usage Guidelines		er group assignment is preve	ser group associated with a task group t enting you from using a command, cont	
Task ID	Task Ope ID	rations		
	interface read	l		
Examples	flushes comm	hand, which displays details	from the show spanning-tree repag t on the MSTIs : g-tree repag b topology-change f.	
		col Instance b	g 0100 10pag 2 00p010gg 0nango 1.	
	Interface	Last TC	Reason	Count
	Gi0/0/0/1	10,00,04,000,07,14		
	Gi0/0/0/1 Gi0/0/0/2		Gi0/0/0/1.10 egress TCN Gi0/0/0/2.1234567890 ingress TCI	65535 N 2
Related Commands				
Related Commands	Gi0/0/0/2 Command	21:05:04 2009-07-15	Gi0/0/0/2.1234567890 ingress TC	N 2
Related Commands	Gi0/0/0/2 Command debug spann 355	21:05:04 2009-07-15	Gi0/0/0/2.1234567890 ingress TCP Description ge Enables Resilient Ethernet Protoco	I (REP) Access Gateway
Related Commands	Gi0/0/0/2 Command debug spann 355 show spanni	21:05:04 2009-07-15	Gi0/0/0/2.1234567890 ingress TCI Description Gebugging commands. Displays the values currently used for by all ports.	I (REP) Access Gateway or populating the BPDUs sent t (bridge ID, cost, and priority)

spanning-tree mst

To enter the MSTP configuration submode, use the **spanning-tree mst** command in global configuration mode.

spanning-tree mst protocol instance identifier

Syntax Description	protocol instance identifier String of a maximum of 25 characters that identifies the protocol instance.			
Command Default	None			
Command Modes	Global config	uration		
Command History	Release	Modification	_	
	Release 3.7.1	This command was introduced.	_	
Usage Guidelines		r group assignment is prevent	group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator	
Note	In MSTP cont	figuration, only one protocol i	nstance can be configured at a time.	
Task ID	Task ID Ope	rations		
	interface read writ	·		
Examples	The following	example shows how to enter	the MSTP configuration submode:	
		PU0:router(config)# spann PU0:router(config-mstp)#	ng-tree mst a	
Related Commands	Command		Description	
	debug spann 345	ing-tree mst packet, on page	Enables debugging for sent and received MSTP packets.	
	debug spann page 347	ng-tree mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.	
	instance (MS	TP), on page 368	Enters the multiple spanning tree instance (MSTI) configuration submode.	

I

Command	Description
interface (MSTP), on page 373	Enters the MSTP interface configuration submode, and enables STP for the specified port.
mvrp static, on page 387	Enables Multiple VLAN Registration Protocol (MVRP) in static mode.
show spanning-tree mst, on page 415	Displays the multiple spanning tree protocol status information.

spanning-tree mstag

To enter the MST Access Gateway configuration submode, use the **spanning-tree mstag** command in global configuration mode.

spanning-tree mstag protocol instance identifier

Syntax Description	protocol instance identifier String of a maximum of 25 characters that identifies the protocol instance.		
Command Default	None		
Command Modes	Global configuration		
Command History	Release Modification		
	Release 3.7.1 This command was introduced.		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
	Refer to the Implementing Multiple Spanning Tree Protocol module of the Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide for more information.		
Note	Unlike MSTP configuration, multiple MSTAG instances can be configured concurrently.		
Task ID	Task ID Operations		
	interface read, write		
Examples	The following example shows how to enter the MSTAG configuration submode.		

RP/0/RSP0/CPU0:router(config)# spanning-tree mstag a
RP/0/RSP0/CPU0:router(config-mstag)#

Related Commands	Command	Description
	debug spanning-tree mstag packet, on page 348	Enables MSTAG packet debugging.
	interface (MSTAG/REPAG), on page 371	Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	instance (MSTAG/REPAG), on page 367	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.

spanning-tree pvrst

To enter the Per VLAN Rapid Spanning Tree (PVRST) configuration submode, use the **spanning-tree pvrst** command in global configuration mode. To exit from the PVRST configuration mode, use the **no** form of this command.

spanning-tree pvrst protocol instance identifier no spanning-tree pvrst protocol instance identifier

Syntax Description	protocol instance identifier String of a maximum of 25 characters that identifies the protocol instance.		
Command Default	None		
Command Modes	Global configu	ration	
Command History	Release N	Iodification	
	Release 5.1 T	his command ntroduced.	l was
Usage Guidelines			nust be in a user group associated with a task group that includes appropriate task ment is preventing you from using a command, contact your AAA administrator
Task ID	Task ID	Operations	
	ethernet-service	es read, write	
Examples	This example s	shows how to	enter the PVRST configuration submode:

RP/0/RSP0/CPU0:router(config)# spanning-tree pvrst st1 RP/0/RSP0/CPU0:router(config-pvrst)#

Related Commands	Comman

Command	Description
forward-delay (PVRST), on page 361	Sets the forward-delay time for the bridge.
interface (PVRST), on page 374	Enables and configures Per VLAN Rapid Spanning Tree (PVRST) on an interface.
maximum (PVRST), on page 384	Sets the maximum age for the bridge.
transmit (PVRST), on page 450	Sets the transmit hold count performance parameter.
vlan (PVRST), on page 453	Configures Per VLAN Rapid Spanning Tree (PVRST) on a VLAN.

spanning-tree pvrstag

To enter the Per VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) configuration submode, use the **spanning-tree pvrstag** command in global configuration mode.

spanning-tree pvrstag protocol instance identifier

Syntax Description	protocol instance identifier String of a maximum of 255 characters that identifies the protocol instance.		
Command Default	None		
Command Modes	Global configu	ration	
Command History	Release	Modification	
		This command was introduced.	
Usage Guidelines		· · ·	in a user group associated with a task group that includes appropriate task s preventing you from using a command, contact your AAA administrator
	-	е .	Spanning Tree Protocol module of the Cisco ASR 9000 Series Aggregation net Services Configuration Guide for more information.
Task ID	Task ID	Operations	
	ethernet-service	s read, write	
Examples	The following o	example shows how	v to enter the PVRSTAG configuration submode:

RP/0/RSP0/CPU0:router(config)# spanning-tree pvrstag a
RP/0/RSP0/CPU0:router(config-pvrstag)#

Related Commands	Command	Description
	debug spanning-tree pvrstag packet, on page 352	Enables packet debugging for sent and received PVRSTAG packets.
	interface (PVSTAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
	show spanning-tree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
	vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.

spanning-tree pvstag

To enter the Per VLAN Spanning Tree Access Gateway (PVSTAG) configuration submode, use the **spanning-tree pvstag** command in global configuration mode.

spanning-tree pvstag protocol instance identifier

Syntax Description	protocol instance identifier String of a maximum of 255 characters that identifies the protocol instance.		
Command Default	None		
Command Modes	Global configu	uration	
Command History	Release	Modification	
	Release 4.0.0	This command introduced.	was
Usage Guidelines			t be in a user group associated with a task group that includes appropriate task ant is preventing you from using a command, contact your AAA administrator
			<i>iple Spanning Tree Protocol</i> module of the <i>Cisco ASR 9000 Series Aggregation</i> <i>hernet Services Configuration Guide</i> for more information.
Task ID	Task ID	Operations	
	ethernet-servi	ces read, write	

Examples The following example shows how to enter the PVSTAG configuration mode:

RP/0/RSP0/CPU0:router(config) # spanning-tree pvstag a
RP/0/RSP0/CPU0:router(config-pvstag) #

Command	Description
debug spanning-tree pvstag packet, on page 354	Enables packet debugging for sent and received PVSTAG packets.
interface (PVSTAG/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
show spanning-tree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
vlan, on page 452	Enables a PVST or PVRST VLAN instance on the interface and enters PVSTAG or PVRSTAG VLAN configuration mode.
	debug spanning-tree pvstag packet, on page 354 interface (PVSTAG/PVRSTAG), on page 375 show spanning-tree pvstag, on page 436

spanning-tree repag

To enter the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode, use the **spanning-tree repag** command in global configuration mode.

spanning-tree repag protocol instance identifier

Syntax Description	protocol instance identifier String of a maximum of 255 characters that identifies the protocol instance.		
Command Default	None		
Command Modes	Global configu	uration	
Command History	Release	Modification	-
	Release 3.7.1	This command was introduced.	-
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.		
			<i>Tree Protocol</i> module of the <i>Cisco ASR 9000 Series Aggregation s Configuration Guide</i> for more information.

Task ID	Task ID	Operations			
	interface	read, write			
Examples	The following example shows how to enter the REPAG configuration mode:				
		P0/CPU0:router(config)# spann P0/CPU0:router(config-repag)#	ing-tree repag a		
Related Commands	Comma	nd	Description		
	debug s 355	panning-tree repag packet, on page	· · · · · · · · · · · · · · · · · · ·		
	355	panning-tree repag packet, on page e (MSTAG/REPAG), on page 371	Enables Resilient Ethernet Protocol (REP) Access Gateway		
	355 interfac		Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands. Enter the MSTAG interface configuration submode, and enables		

track

To enter the MSTAG uplink tracking submode, use the **track** command in MST Access Gateway configuration submode.

	track		
Syntax Description	track Enters the MSTAG uplink tracking submode.		
Command Default	None		
Command Modes	MST Access Gateway configuration submode		
Command History	Release	Modification	
	Release 6.2.2	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.		
			ree Protocol module of the Cisco ASR 9000 Series Aggregation Configuration Guide for more information.

I

Task ID	Task ID Operations				
	interface read, write				
Examples	The following example shows how to enter the MSTAG uplink tracking submode configuration submode.				
	RP/0/RSP0/CPU0:router(config-mstag RP/0/RSP0/CPU0:router(config-mstag				
Related Commands	Command	Description			
	interface (MSTAG Uplink Tracking), on page 376				
	spanning-tree mstag, on page 444	Enters the MST Access Gateway configuration submode.			
	show spanning-tree mstag tracked, on p	age 431 Displays the core connectivity tracking data.			
	show spanning-tree mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.			

transmit (PVRST)

To set the transmit hold count performance parameter, use the **transmit** command in PVRST configuration submode. To undo the setting, use the **no** form of this command.

transmit hold-count count no transmit hold-count count

Syntax Description	hold-count		Specifies the hold count performance parameter of the bridge.
	count		Bridge transmit hold count. The range is from 1 to 10.
Command Default	None		
Command Modes	PVRST con	figuration	
Command History	Release	Modification	
	Release 5.1	This command was introduced.	

To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. Task ID Task ID Operations ethernet-services read, write Examples This example shows how to set the bridge transmit hold-count parameter to 8: RP/0/RSP0/CPU0:router(config) # spanning-tree pvrst st1 RP/0/RSP0/CPU0:router(config-pvrst)# transmit hold-count 8 **Related Commands** Command Description Sets the forward-delay time for the bridge. forward-delay (PVRST), on page 361 Enables and configures Per VLAN Rapid Spanning Tree (PVRST) interface (PVRST), on page 374 on an interface. maximum (PVRST), on page 384 Sets the maximum age for the bridge. Configures Per VLAN Rapid Spanning Tree (PVRST) on a VLAN. vlan (PVRST), on page 453

transmit hold-count

To set the transmit hold count performance parameter, use the **transmit hold-count** command in MSTP configuration submode.

	transmit hold-count count		
Syntax Description	count Bridge	transmit hold count. Range is	1 to 10.
Command Default	<i>count:</i> 6		
Command Modes	MSTP configuration		
Command History	Release	Modification	
	Release 3.7.1	This command was introduced.	
Usage Guidelines		r group assignment is preven	group associated with a task group that includes appropriate task ing you from using a command, contact your AAA administrator

Task ID	Task ID	Operations		
	interface	read, write	-	
Examples	The follow	ving exam	ple shows how to set the b	ridge transmit hold-count parameter to 8:
			uter(config)# spanning uter(config-mstp)# tra	
Related Commands	Command	1		Description
	debug sp	anning-tre	e mst packet, on page 345	Enables debugging for sent and received MSTP packets.
	debug sp page 347	anning-tre	e mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.
	spanning	-tree mst, o	on page 443	Enters the MSTP configuration submode
	show spanning-tree mst, on page 415			Displays the multiple spanning tree protocol status information.
vlan		tion mode,		on the interface and enter PVSTAG or PVRSTAG VLAN PVSTAG or PVRSTAG configuration submode.
Syntax Description	vlan-id S	Specifies th	e VLAN identifier. The ra	nge of the VLAN ID is between 1 to 4094.
	Note There is a limit of 200 VLANs per physical interface and 16000 VLANs across the system.			
Command Default	None			
Command Modes	PVRSTAG	G interface	configuration, PVSTAG i	nterface configuration
Command History	Release	Modi	fication	
	Release 4		command was duced.	
Usage Guidelines		user group		oup associated with a task group that includes appropriate task you from using a command, contact your AAA administrator

-		
Task ID	Operations	
ethernet-services	read, write	
The following exa	mple shows how to enabl	e a VLAN in the PVSTAG configuration mode:
RP/0/RSP0/CPU0: RP/0/RSP0/CPU0:	router(config-pvstag); router(config-pvstag-:	<pre># interface GigabitEthernet 0/3/03 if)# vlan 100</pre>
Command		Description
debug spanning-t page 352	tree pvrstag packet, on	Enables packet debugging for sent and received PVRSTAG packets.
debug spanning-t 354	ree pvstag packet, on page	Enables packet debugging for sent and received PVSTAG packets.
interface (PVSTA	G/PVRSTAG), on page 375	Enters PVST or PVRST Access Gateway Interface configuration submode and enables either PVSTAG or PVRSTAG for the specified port.
show spanning-ti	ree pvrstag, on page 435	Displays the values currently used for populating the BPDUs sent by all ports.
show spanning-t	ree pvstag, on page 436	Displays the values currently used for populating the BPDUs sent by all ports.
spanning-tree pv	rstag, on page 446	Enters the Per VLAN Rapid Spanning Tree Access Gateway
		(PVRSTAG) configuration submode.
	ethernet-services The following exa RP/0/RSP0/CPU0: RP/0/RSP0/CPU0: RP/0/RSP0/CPU0: Command debug spanning-t page 352 debug spanning-t 354 interface (PVSTA show spanning-tu	ethernet-services read, write The following example shows how to enable RP/0/RSP0/CPU0:router(config) # spann: RP/0/RSP0/CPU0:router(config-pvstag); RP/0/RSP0/CPU0:router(config-pvstag); RP/0/RSP0/CPU0:router(config-pvstag); RP/0/RSP0/CPU0:router(config-pvstag); RP/0/RSP0/CPU0:router(config-pvstag); RP/0/RSP0/CPU0:router(config-pvstag); RP/0/RSP0/CPU0:router(config-pvstag); RP/0/RSP0/CPU0:router(config-pvstag); Image 352 debug spanning-tree pvrstag packet, on page 354 interface (PVSTAG/PVRSTAG), on page 375 show spanning-tree pvrstag, on page 435 show spanning-tree pvstag, on page 436

vlan (PVRST)

To configure Per VLAN Rapid Spanning Tree (PVRST) on a VLAN, use the **vlan** command in PVRST configuration submode. To undo the configuration, use the **no** form of this command.

vlan vlan-id priority bridge-priority no vlan vlan-id priority bridge-priority

		VLAN ID. The range is from 1 to 4094.
pr	iority	Specifies the bridge priority.
bri	idge-priority	Bridge priority. The value is a multiple of 4096.

Command Default None

Command Modes	PVRST confi	guration			
Command History	Release	Modification			
		This command was introduced.			
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.				
	01	· ·	, and the valid range is 0 to 61440. Allowed values are: 0 4096 8192 36864 40960 45056 49152 53248 57344 61440.		
Task ID	Task ID	Operations			
	ethernet-servic	ces read, write			
Examples	This example shows how to use the vlan-id command:				
		PU0:router(config)# spa PU0:router(config-pvrst	nning-tree pvrst stl)# vlan 66 priority 4096		
Related Commands	Command		Description		
	forward-dela	y (PVRST), on page 361	Sets the forward-delay time for the bridge.		
	interface (PV	(RST), on page 374	Enables and configures Per VLAN Rapid Spanning Tree (PVRST) on an interface.		
	maximum (P\	/RST), on page 384	Sets the maximum age for the bridge.		
	transmit (PVF	RST), on page 450	Sets the transmit hold count performance parameter.		

vlan-ids (MSTAG/REPAG)

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

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

Syntax Description	<i>vlan-range</i> List of VLAN ranges in the form a-b, c, d, e-f, g etc.
Command Default	None
Command Modes	MSTAG Instance configuration mode, REPAG Instance configuration mode.

Command History	Release	Modi	fication	_
	Release 3.	.7.1 This c introd	command was luced.	_
Usage Guidelines		user group		roup associated with a task group that includes appropriate task ag you from using a command, contact your AAA administrator
Task ID	Task ID	Operations		
	interface	read, write		
Examples	The follow	ving examp	ble shows how to use the	vlan-id command:
	RP/0/RSP0	/CPU0:rou	iter(config-mstag-ins	st)# vlan-id 2-1005
Related Commands	Command			Description
	debug spa 348	anning-tree	e mstag packet, on page	Enables MSTAG packet debugging.
	debug spanning-tree repag packet, on page 355			Enables Resilient Ethernet Protocol (REP) Access Gateway debugging commands.
	interface (MSTAG/REPAG), on page 371			Enter the MSTAG interface configuration submode, and enables MSTAG for the specified port.
	instance (MSTAG/RE	PAG), on page 367	Enters MSTAG Instance configuration mode or REPAG Instance configuration mode.
	spanning-	tree mstag	I, on page 444	Enters the MST Access Gateway configuration submode.
	spanning-	tree repag	, on page 448	Enters the Resilient Ethernet Protocol Access Gateway (REPAG) configuration submode.
	show spa	nning-tree	mstag, on page 426	Displays the values currently used for populating the BPDUs sent by all ports.
	show spa	nning-tree	repag, on page 438	Displays the values currently used for populating the BPDUs sent by all ports.

vlan-id (MSTP)

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

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

I

Syntax Description	vlan-rang	<i>vlan-range</i> List of VLAN ranges in the form a-b, c, d, e-f, g etc.		
Command Default	None			
Command Modes	MSTI con	figuration		
Command History	Release	Modification		
	Release 3	.7.1 This command was introduced.		
Usage Guidelines		user group assignment is preventing	oup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator	
Task ID	Task ID	Operations		
	interface	read, write		
Examples	The following example shows how to use the vlan-id command:			
	RP/0/RSP(0/CPU0:router(config-mstp-inst))# vlan-id 2-1005	
Related Commands	Command	d	Description	
	debug sp	anning-tree mst packet, on page 345	Enables debugging for sent and received MSTP packets.	
	debug sp page 347	anning-tree mst protocol-state, on	Enables debugging protocol-state changes such as port role or state changes, topology change notification.	
	instance	(MSTP), on page 368	Enters the multiple spanning tree instance (MSTI) configuration submode.	
	spanning	-tree mst, on page 443	Enters the MSTP configuration submode	



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 457
- deny (ES ACL), on page 459
- ethernet-service access-group, on page 461
- ethernet-services access-list, on page 462
- permit (ES ACL), on page 464
- resequence access-list ethernet-service, on page 466
- show access-lists ethernet-services, on page 468
- show access-lists ethernet-services trace, on page 471
- show access-list ethernet-service usage pfilter, on page 473
- show lpts pifib hardware entry optimized, on page 474

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-n	st ethernet-service source-act	aestination-aci
Syntax Description	source-acl	Name of the access list to be c	opied.
	destination-ac	<i>l</i> Name of the destination access	list where the contents of the <i>source-acl</i> argument is copied.
Command Default	None		
Command Modes	EXEC		
Command History	Release	Modification	
		This command was introduced.	

conv access-list ethernet-service source-acl destination-acl

To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** 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 C

ed Commands	Command	Description	
	deny (ES ACL), on page 459	Sets conditions for an Ethernet services access list	
	ethernet-service access-group, on page 461	Controls access to an interface.	
	ethernet-services access-list, on page 462	Defines an Ethernet services (Layer 2) access list by name.	
	permit (ES ACL), on page 464	Sets conditions for an Ethernet services access list.	
	resequence access-list ethernet-service, on page 466	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.	
	show access-lists ethernet-services, on page 468	Displays the contents of current Ethernet services access lists.	
	show access-lists ethernet-services trace, on page 471	Displays Ethernet services access list trace information.	
	show access-list ethernet-service usage pfilter, on page 473	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	<i>sequence-number</i> (Optional) Number of the deny statement in the access list. This number deter order of the statements in the access list. The number can be from 1 to 214748 default, the first statement is number 10, and the subsequent statements are ind by 10.) Use the resequence access-list ethernet-service command to change the of the first statement and increment subsequent statements of a configured acc			
	src-mac-address	Source MAC address in format <i>H.H.H.</i>		
	src-mac-mask	Source MAC mask in format <i>H.H.H.</i>		
	any	Denies any source MAC address and mask.		
	host	Denies host with a specific host source MAC address and mask, in format <i>H.H.H.</i>		
	dest-mac-address	Destination MAC address in format <i>H.H.H.</i>		
	dest-mac-mask	Destination MAC mask in format <i>H.H.H.</i>		
	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.		

I

Command Modes Ethernet services access list configuration Release Modification 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 tast Dbs. If the user group assignment is preventing you from using a command, contact your AAA administrato 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 consecutively numbered statements (for example, between line 10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the firs statement and increment the entry number of each subsequent statement. Task ID Task Operations ID acl read, write Examples The following example shows how to define an Ethernet services access-list L2ACL1 %///KSPO/CPU0:router(config1= ethernet-services access-list L2ACL1 %///KSPO/CPU0:router(config1=ethernet-services access-list L2ACL1 %//KSPO/CPU0:router(config1=ethernet-services access-list L2ACL1 %//KSPO/CPU0:router(config1=ethernet-services access-list L2ACL						
Command Default There is no default condition under which a packet is denied passing the Ethernet services access list. Command Mades Ethernet services access list configuration 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 tast IDs. If the user group assignment is preventing you from using a command, contact your AAA administrato 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 fails between two consecutively numbered statements. If you want to add a statement between two consecutively numbered statements. If you want to add a statement there entry number of each subsequent statement. Task ID Task Operations ID Task Operations ID Task Operations ID Task (CONTROL/CEDD) (CEDD) (CEDD		cos-value	Inner header class of service	value. Range is from 0 to 7.		
Command Modes Ethemet services access list configuration Release Modification Release Addition 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 tast IDs. If the user group assignment is preventing you from using a command, contact your AAA administrato 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 consecutively numbered statements (for example, between line 10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the firs statement and increment the entry number of each subsequent statement. Task ID Task Operations 10 acl read, write Examples The following example shows how to define an Ethernet services access list named L2ACL1: R2/0/R3P0/CPU0:router(config) # ethernet-services access list named L2ACL1: R2/0/R3P0/CPU0:router(config) = ethernet-services access list named L2ACL1 R2/0/R3P0/CPU0:router(config) = ethernet-services access list named L2ACL1 R2/0/R3P0/CPU0:router(config====1) # 30 permit 00ff.eed.0010 ff100 000.00ff 0011.eb10.		inner-dei	(Optional) Denies based on i	nner header discard eligibility indicator.		
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 administrato 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 that falls between two consecutively numbered statements (for example, between line 10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the first statement and increment the entry number of each subsequent statement. Task ID Task Operations access list in the entry exvices access list named L2ACL1: RP/0/R3P0/CP00:router(config) # ethernet-services access list named L2ACL1:	Command Default	There is no defa	ult condition under which a pack	xet is denied passing the Ethernet services access list.		
Release 3.7.2 This command was introduced. Usage Guidelines Do use this command, you must be in a user group associated with a task group that includes appropriate tast Do. If the user group assignment is preventing you from using a command, contact your AAA administrato 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 consecutively numbers to indicate where it belongs. If you want to add a statement between two consecutively numbered statements (for example, between line 10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the firs statement and increment the entry number of each subsequent statement. Task ID Task Operations ID acl read, write Examples The following example shows how to define an Ethernet services access list named L2ACL1: REP/0/RSP0/CPD0 irouter (config) + ethernet-services access-list 12ACL1 REP/0/RSP0/CPD0 irouter (config-es-acl) + 10 permit 00ff.eedd.0010 ff00.0000.00ff 0011.ab10.eder ffff.0000.ff00 vlan 1000-1100 inner-vlan 100 inner-vcos 7 inner-dei REV/0/RSP0/CPD0 irouter (config-es-acl) + 30 permit 00ff eedd.0011.ff1c ff001.0000.00ff any vlan SP0/0 cos 1 inner-vlan 30 inner-vcos 6 REV/0/RSP0/CPD0 irouter (config-es-acl) + 30 permit any any vlan 500 cos	Command Modes	Ethernet service	es access list configuration			
introduced. Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate tast IDs. If the user group assignment is preventing you from using a command, contact your AAA administrate for assistance. Use the demy 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 consecutively numbered statements (for example, between line 10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the first statement and increment the entry number of each subsequent statement. Task ID Task Operations ID acl read, write Examples The following example shows how to define an Ethernet services access-list L2ACL1 RP/0/RSPO/CPU0:router(config) # ethernet-services access-list L2ACL1 RP/0/RSPO/CPU0:router(config) # othernet-services access-list L2ACL1 RP/0/RSPO/CPU0:router(config) # othernet-services access-list L2ACL1 RP/0/RSPO/CPU0:router(config) # othernet-services access-list C2ACL1 RP/0/RSPO/CPU0:router(config) # othernet-services access-list L2ACL1	Command History	Release	Modification			
IDs. If the user group assignment is preventing you from using a command, contact your AAA administrato 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 line 10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the first statement and increment the entry number of each subsequent statement. Task ID Task Operations ID acl read, write Examples The following example shows how to define an Ethernet services access list named L2ACL1: RP/0/R8P0/CPU0:router (config)# ethernet-services access-list L2ACL1 RP/0/R8P0/CPU0:router(config-es-acl)# 10 permit 00ff.edd.0010 ff00.0000.00ff 0011.ab10.cder fffff.0000.ff00 v1an 1000-1100 inner-val= 100 RP/0/R8P0/CPU0:router (config-es-acl)# 20 deny host eedd.0011.fflc ff00.0000.00ff any vlan 300 cos 1 dei inner-vlan 30 inner-vals 6 RP/0/R8P0/CPU0:router (config-es-acl)# 30 permit any any vlan 500 cos 2 inner-vlan 600 inner-cos 5 inner-dei Related Commands						
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 line 10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the first statement and increment the entry number of each subsequent statement. Task ID Task Operations ID acl read, write Examples The following example shows how to define an Ethernet services access list named L2ACL1: RP/0/RSP0/CP00:router(config) # ethernet-services access-list 12ACL1 RP/0/RSP0/CP00:router(config-es-acl) # 10 permit 00ff.eed.0010 ff00.0000.00ff 0011.ab10.cde: ffff.0000.0ff0 vlan 1000-1100 inner-cos 7 inner-dei RP/0/RSP0/CP00:router(config-es-acl) # 20 deny host eedd.0011.fflc ff00.0000.0ff any vlan 300 cos 1 dei inner-vlan 30 inner-cos 6 RP/0/RSP0/CP00: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 457 Creates a copy of an existing Ethernet services access list	Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.				
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 line 10 and 11), first use the resequence access-list ethemet-service, on page 466 command to renumber the first statement and increment the entry number of each subsequent statement. Task ID Task Operations ID 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.cde: ffff.000.0000.00ff 0011.ab10.cde: ffff.000.0000.00ff onl.ab10.cde: ffff.000.0000.00ff onl and 100 inner-cos 7 inner-dei 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 457 Creates a copy of an existing Ethernet services access list			-	service access-list command to specify conditions under		
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 line 10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the first statement and increment the entry number of each subsequent statement. Task ID Task Operations ID 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.cdest 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 Related Commands Command Description		By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.				
10 and 11), first use the resequence access-list ethernet-service, on page 466 command to renumber the first statement and increment the entry number of each subsequent statement. Task ID Task Operations ID acl read, write acl read, evrite 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.cde: 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 457 Creates a copy of an existing Ethernet services access list		new statement anywhere other than at the end of the list, create a new statement with an appropriate entry				
ID 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.cdes 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 457 Creates a copy of an existing Ethernet services access list		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 466 command to renumber the first				
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.cdes 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.fflc 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 457 Creates a copy of an existing Ethernet services access list	Task ID	-	ns			
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.cdes 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 457 Creates a copy of an existing Ethernet services access list		,				
RP/0/RSP0/CPU0:router(config-es-acl)# 10 permit 00ff.eedd.0010 ff00.0000.00ff 0011.ab10.cde: 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 Description copy access-list ethernet-service, on page 457 Creates a copy of an existing Ethernet services access list	Examples	The following example shows how to define an Ethernet services access list named L2ACL1:				
copy access-list ethernet-service, on page 457 Creates a copy of an existing Ethernet services access list		RP/0/RSP0/CPU ffff.0000.ff RP/0/RSP0/CPU 300 cos 1 de RP/0/RSP0/CPU	0:router(config-es-acl)# 10 p 00 vlan 1000-1100 inner-vla 0:router(config-es-acl)# 20 i inner-vlan 30 inner-cos 6 0:router(config-es-acl)# 30	permit 00ff.eedd.0010 ff00.0000.00ff 0011.ab10.cdef an 100 inner-cos 7 inner-dei deny host eedd.0011.ff1c ff00.0000.00ff any vlan		
	Related Commands	Command		Description		
ethernet-service access-group, on page 461 Controls access to an interface.		copy access-li	st ethernet-service, on page 457	Creates a copy of an existing Ethernet services access list.		
		ethernet-servic	ce access-group, on page 461	Controls access to an interface.		

Command	Description
ethernet-services access-list, on page 462	Defines an Ethernet services (Layer 2) access list by name.
permit (ES ACL), on page 464	Sets conditions for an Ethernet services access list.
resequence access-list ethernet-service, on page 466	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 468	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 471	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 473	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 command.	access list as specified by the ethernet-service access-list	
	ingress	gress Filters on inbound packets.		
	egress	Filters on outbound packets.		
Command Default	The interface doe	es not have an Ethernet services	access list applied to it.	
Command Modes	Interface configuration			
Command History	Release N	lodification		
		his command was attroduced.		
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.			
	access group, use	e the no form of the command. I st. Use the ingress keyword to	In the control access to an interface. To remove the specified Use the <i>acl-name</i> argument to specify a particular Ethernet filter on inbound packets or the egress keyword to filter on	

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 ID

 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 457	Creates a copy of an existing Ethernet services access list.
	deny (ES ACL), on page 459	Sets conditions for an Ethernet services access list
	ethernet-services access-list, on page 462	Defines an Ethernet services (Layer 2) access list by name.
	permit (ES ACL), on page 464	Sets conditions for an Ethernet services access list.
	resequence access-list ethernet-service, on page 466	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
	show access-lists ethernet-services, on page 468	Displays the contents of current Ethernet services access lists.
	show access-lists ethernet-services trace, on page 471	Displays Ethernet services access list trace information.
	show access-list ethernet-service usage pfilter, on page 473	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 marks, but can include numbe	access list. The name cannot contain a spaces or quotation rs.
Command Default	No Ethernet serv	ices access list is defined.	
Command Modes	Global configura	tion	
Command History	Release M	lodification	
		his command was troduced.	
Usage Guidelines			o associated with a task group that includes appropriate task ou from using a command, contact your AAA administrator
		-	es the router in access list configuration mode, in which the ned with the deny (ES ACL) or permit (ES ACL) command.
	-		n page 466 command if you need to add a permit or deny ing Ethernet services access lists.
Task ID	Task Operations	S	
	acl read, write	_	
Examples	The following ex	ample shows how to define an I	Ethernet services access list named L2ACL1:
	RP/0/RSP0/CPU0	:router(config)# ethernet-s	ervices access-list L2ACL1
Related Commands	Command		Description
	copy access-list	ethernet-service, on page 457	Creates a copy of an existing Ethernet services access list.
	deny (ES ACL), o	n page 459	Sets conditions for an Ethernet services access list
	ethernet-service	access-group, on page 461	Controls access to an interface.
	permit (ES ACL),	on page 464	Sets conditions for an Ethernet services access list.
	resequence acce 466	ess-list ethernet-service, on page	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
	show access-list	s ethernet-services, on page 468	Displays the contents of current Ethernet services access lists.
	show access-lis page 471	ts ethernet-services trace, on	Displays Ethernet services access list trace information.

Command	Description
show access-list ethernet-service usage pfilter, on page 473	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

S

_	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 <i>H.H.H.</i>
	src-mac-mac	Source MAC mask in format <i>H.H.H.</i>
	any	Permits any source MAC address and mask.
	host	Permits host with a specific host source MAC address and mask, in format <i>H.H.H.</i>
	dest-mac-address	Destination MAC address in format <i>H.H.H.</i>
	dest-mac-mac	Destination MAC mask in format <i>H.H.H.</i>
	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 spec	ific default condition under which a packet is permitted passing the Ethernet services ACL.
Command Modes	Ethernet services	s access list configuration
Command History	Release N	Nodification
		This command was ntroduced.
Usage Guidelines		nand, you must be in a user group associated with a task group that includes appropriate task group assignment is preventing you from using a command, contact your AAA administrator
	-	command following the ethernet-service access-list command to specify conditions under can pass the access list.
	By default, the factor by 10.	irst statement in an access list is number 10, and the subsequent statements are incremented
	new statement a	mit or deny statements to an existing access list without retyping the entire list. To add a nywhere other than at the end of the list, create a new statement with an appropriate entry between two existing entry numbers to indicate where it belongs.
	10 and 11), first	Id a statement between two consecutively numbered statements (for example, between lines use the resequence access-list ethernet-service, on page 466 command to renumber the first crement the entry number of each subsequent statement.
Task ID	Task Operation ID	 IS
	acl read, write	_
Examples	The following ex	xample show how to set a permit condition for an access list named L2ACL1:
	RP/0/RSP0/CPU0 ffff.0000.ff0 RP/0/RSP0/CPU0	<pre>D:router(config)# ethernet-services access-list L2ACL1 D:router(config-es-al)# 10 permit 00ff.eedd.0010 ff00.0000.00ff 0011.ab10.cdef 00 vlan 1000-1100 inner-vlan 100 inner-cos 7 inner-dei D:router(config-es-al)# 20 permit any host 000a.000b.000c 0800 vlan 500 cos 2 00 inner-cos 5 inner-dei</pre>

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 457	Creates a copy of an existing Ethernet services access list.
	deny (ES ACL), on page 459	Sets conditions for an Ethernet services access list
	ethernet-service access-group, on page 461	Controls access to an interface.
	ethernet-services access-list, on page 462	Defines an Ethernet services (Layer 2) access list by name.
	resequence access-list ethernet-service, on page 466	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
	show access-lists ethernet-services, on page 468	Displays the contents of current Ethernet services access lists.
	show access-lists ethernet-services trace, on page 471	Displays Ethernet services access list trace information.
	show access-list ethernet-service usage pfilter, on page 473	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: increment: 10	10
Command Modes	- EXEC	

Command History	Release	Modification		
	Release 3.7	2.2 This command was introduced.		
Usage Guidelines		ser group assignment is preventing years	p associated with a task group that includes appropriate task ou from using a command, contact your AAA administrator	
	consecutive start-sequer	entries in an existing Ethernet servic <i>ace-number</i>) and the increment by wh nembers the existing statements, ther	command to add a permit or deny statement between es access list. Specify the first entry number (the ich to separate the entry numbers of the statements. the eby making room to add new statements with the unused	
Task ID	Task Ope ID	erations		
	acl read wri			
Examples	In the following example, suppose you have an existing access list:			
	10 permi 20 deny	ervice access-list L2ACL1 t 1.2.3 4.5.6 2.3.4 5.4.3 t 3.1.2 5.3.4 cos 5		
	resequence	the entries, renumbering the statemen	ist ahead of the first permit statement. First, you ts starting with number 20 and an increment of 10, s 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			
	20 permi 30 deny	ervice access-list L2ACL1 t 1.2.3 4.5.6 2.3.4 5.4.3 t 3.1.2 5.3.4 cos 5		
Related Commands	Command		Description	
	copy acces	ss-list ethernet-service, on page 457	Creates a copy of an existing Ethernet services access list.	
	deny (ES A	CL), on page 459	Sets conditions for an Ethernet services access list	
	ethernet-se	ervice access-group, on page 461	Controls access to an interface.	
		1	Define a su Ethermot a su i a su (la su a 2) a su a su list have su a	

VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers, IOS XR Release 6.4.x

ethernet-services access-list, on page 462

permit (ES ACL), on page 464

Defines an Ethernet services (Layer 2) access list by name.

Sets conditions for an Ethernet services access list.

Command	Description
show access-lists ethernet-services, on page 468	Displays the contents of current Ethernet services access lists.
show access-lists ethernet-services trace, on page 471	Displays Ethernet services access list trace information.
show access-list ethernet-service usage pfilter, on page 473	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		ser group assignment is preventing	roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator	
Task ID	Task Oper ID	ations		
	acl read write	·		
Examples	The followin	ng examples lists defined Etherner	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/RSP0/0	CPU0:router# show access-lis	ts ethernet-services standby	
	10 permit ethernet-se 10 permit	ervices access-list i host 0001.0002.0003 host 00 ervices access-list 12_acl any any ost 0002.0003.0004 host 000.		
	-		The number of Ethernet services ACLs configured on	
	RP/0/RSP0/0	CPU0:router# show access-lis	ts ethernet-services summary	
		y: Ls configured: 2 Es configured: 3		
	The followin	g example displays the number of	Enackets matching the access list 12 acl for each ACE.	

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 12_ACL hardware ingress location 0/0/CPU0

ethernet service access-list 12_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 12_acl:

RP/0/RSP0/CPU0:router# show access-lists ethernet-services 12_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 12_ACL hardware ingress sequence
20 location 0/0/CPU0
```

```
ethernet-services access-list 12_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: 12acl 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
-----Field Details-----
                 : 0000
outer vlan id value
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
                 : 0001
Base acl id value
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
RP/0/RSP0/CPU0:router#

Related Commands	Command	Description
	copy access-list ethernet-service, on page 457	Creates a copy of an existing Ethernet services access list.
	deny (ES ACL), on page 459	Sets conditions for an Ethernet services access list
	ethernet-service access-group, on page 461	Controls access to an interface.
	ethernet-services access-list, on page 462	Defines an Ethernet services (Layer 2) access list by name.
	permit (ES ACL), on page 464	Sets conditions for an Ethernet services access list.
	resequence access-list ethernet-service, on page 466	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
	show access-lists ethernet-services trace, on page 471	Displays Ethernet services access list trace information.
	show access-list ethernet-service usage pfilter, on page 473	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 failu	res.
	critical	Trace data for server-critical fat	ilures
	both	Trace data for server-critical and	l intermittent failures.
	all	Trace data for server-critical and	l intermittent failures.
Command Modes	EXEC		
Command History	Release	Modification	
	Release 3.7.2	This command was introduced.	

To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. Task ID Task Operations ID 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 Creates a copy of an existing Ethernet services access list. copy access-list ethernet-service, on page 457 Sets conditions for an Ethernet services access list deny (ES ACL), on page 459

ethernet-service access-group, on page 461Controls access to an interface.ethernet-services access-list, on page 462Defines an Ethernet services (Layer 2) access list by name.

Command	Description
resequence access-list ethernet-service, on page 466	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
show access-lists ethernet-services, on page 468	Displays the contents of current Ethernet services access lists.
show access-list ethernet-service usage pfilter, on page 473	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-li	<i>access-list-name</i> (Optional) Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.				
	location	l	Interface card on which the access list information is needed.			
	location		Fully qualified location sp	ecification.		
	all		Displays packet filtering u	sage for all interface cards.		
Command Modes	EXEC					
Command History	Release	Мо	odification	-		
	Release		is command was roduced.	-		
Usage Guidelines		e user gro		roup associated with a task group that includes appropriate task g you from using a command, contact your AAA administrator		
Task ID	Task (ID	Operations	-			
		ead, write	-			
Examples	The follo	owing exa	mple 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 : 12_acl
Output ACL : N/A
Interface : GigabitEthernet0/0/0/30
Input ACL : N/A
Output ACL : N/A
```

The following example shows the results of the command for a specific ACL:

```
RP/0/RSP0/CPU0:router# show access-list ethernet-services 12_acl usage pfilter location
0/0/CPU0
Interface : GigabitEthernet0/0/0/9
Input ACL : 12_acl
Output ACL : N/A
```

Related Commands	Command	Description
	copy access-list ethernet-service, on page 457	Creates a copy of an existing Ethernet services access list.
	deny (ES ACL), on page 459	Sets conditions for an Ethernet services access list
	ethernet-service access-group, on page 461	Controls access to an interface.
	ethernet-services access-list, on page 462	Defines an Ethernet services (Layer 2) access list by name.
	permit (ES ACL), on page 464	Sets conditions for an Ethernet services access list.
	resequence access-list ethernet-service, on page 466	Renumbers existing statements and increment subsequent statements to allow a new Ethernet services access list statement.
	show access-lists ethernet-services, on page 468	Displays the contents of current Ethernet services access lists.
	show access-lists ethernet-services trace, on page 471	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 Operation ID Ipts 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 - I	nterface in opti	mized list	
Protocol	laddr.Port, raddr.Port	Intf	VRF id	State
IGMP	224.0.0.22.any , any.any	Te0/4/0/0 Te0/4/0/1	* *	Uidb Set Uidb Set
	224.0.0.22.any , any.any	Te0/4/0/0 Te0/4/0/1	*	Uidb Set Uidb Set
	any.any , any.any	Te0/4/0/0 Te0/4/0/1	*	Uidb Set Uidb Set

VPN and Ethernet Services Command Reference for Cisco ASR 9000 Series Routers, IOS XR Release 6.4.x



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 477
- interface nve, on page 478
- member, on page 479
- member vni, on page 480
- overlay-encapsulation, on page 481
- show nve interface, on page 482
- show nve peers, on page 483
- show nve vni, on page 484
- source-interface loopback, on page 484

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	Configures loopback interface as the source interface for the VTEP.
	loopback-interface-identifier	The variable <i>loopback-interface-identifier</i> 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 c	ommand.
	This examp	le shows how to configure anycast	mode parameters for VTEP.
		CPU0:router# configure	
		<pre>/CPU0:router(config)# interfa /CPU0:router(config-if)# over</pre>	
		/CPU0:router(config-if)# sour	
			er vni 1 mcast-group 192.20.9.2 0.0.0.0
	RP/0/RSP0/	<pre>/CPU0:router(config-if) # anyca</pre>	st 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** The NVE interface ID. It can take values from 1 to 65535. nve-id None **Command Default Global Configuration Command Modes Command History** Release Modification Release This command was introduced. 5.2.0 To use this command, you must be in a user group associated with a task group that includes appropriate task **Usage Guidelines** 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]

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 end_ip_address The end multicast IP address from a range. Command Default None Command Modes NVE interface configuration Command History Release Modification Release To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor 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 100-120 mcast-group 224.2.2.25 RP/0/RSP0/CPU0:router (config-if) # member vni 100-120 mcast-group 224.2.2.2.55 To use this command, you must be in a user group associated with a task group that incl	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 NVE interface configuration Command History Release Release This command was introduced. 5.2.0 To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step				
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 end_ip_address The end multicast IP address from a range. Command Default None Command Modes NVE interface configuration Command History Release Release This command was introduced. 5.2.0 To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor VXLAN or VXLAN range. For instance, RP/0/RSP0/CPU0:router (config-fif) # member vni 10 mcast-group 224.2.2.10 RP/0/RSP0/CPU0:router (config-fif) # member vni 23 mcast-group 224.2.2.23 RP/0/RSP0/CPU0:router (config-fif) # member vni 10 mcast-group 224.2.2.24 To use this command, you must be in a user group associated with a task group that incl Rest	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 NVE interface configuration Command History Release Modification Release This command was introduced. 5.2.0 To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step	Syntax Description	vni	The member VNI.	
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 end_ip_address The end multicast IP address from a range. Command Default None None NVE interface configuration Command Modes NVE interface configuration Image Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor 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 100-l20 mcast-group 224.2.2.50 RP/0/RSP0/CPU0:router(config-if)# member vni 100-l20 mcast-group 224.2.2.51 To use this command, you must be in a user group associated with a task group that incl	end_number The end VNI from a range. incast-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. end_ip_address The end multicast IP address from a range. Command Default None NVE interface configuration Command History Release Modification Release This command was introduced. 5.2.0 To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step		number	The VNI for a single VXLAN. The valid values are from 1 to 16777215.	
mcast-group The multicast group. ip_address A single multicast IP address or the starting multicast IP address from end_ip_address The end multicast IP address from a range. Command Default None Command Modes NVE interface configuration Command History Release Release This command was introduced. 5.2.0 Solution Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor 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 100-120 mcast-group 224.2.2.50 RP/0/RSP0/CPU0:router(config-if)# member vni 100-120 mcast-group 224.2.2.50 To use this command, you must be in a user group associated with a task group that incl	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 NVE interface configuration NVE interface configuration Release This command was introduced. 5.2.0 To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step		start_number	The first VNI from a range.	
ip_address A single multicast IP address or the starting multicast IP address from end_ip_address Command Default None None NVE interface configuration Command History Release Modification Release To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor 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 224.2.2.3 RP/0/RSP0/CPU0:router (config-if) # member vni 100-120 mcast-group 224.2.2.50 RP/0/RSP0/CPU0:router (config-if) # member vni 100-120 mcast-group 224.2.2.2.50 RP/0/RSP0/CPU0:router (config-if) # member vni 100-120 mcast-group 224.2.2.50 RP/0/RSP0/CPU0:router (config-if) # member vni 100-120 mcast-group 224.2.2.50	ip_address A single multicast IP address or the starting multicast IP address from a range. ip_address The end multicast IP address from a range. command Default None NVE interface configuration NVE interface configuration command History Release Release This command was introduced. 5.2.0 To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step		end_number	The end VNI 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 This command was introduced. 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor 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 224.2.2.55 RP/0/RSP0/CPU0:router (config-if) # member vni 100-120 mcast-group 224.2.2.55 To use this command, you must be in a user group associated with a task group that incl	Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constraint of the end multicast IP address from a range. Image: Constreact IP address from a range. <td></td> <td>mcast-group</td> <td>The multicast group.</td>		mcast-group	The multicast group.	
Command Default None Command Modes NVE interface configuration Command History Release Modification Release This command was introduced. 5.2.0 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor VXLAN or 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 224.2.2.2.3 RP/0/RSP0/CPU0:router (config-if)# member vni 50-59 mcast-group 224.2.2.50 RP/0/RSP0/CPU0:router (config-if)# member vni 100-120 mcast-group 224.2.2.2.10 To use this command, you must be in a user group associated with a task group that incl	Command Default None Command Modes NVE interface configuration Command History Release Modification Release This command was introduced. 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step		ip_address	A single multicast IP address or the starting multicast IP address from a range.	
Command Modes NVE interface configuration Command History Release Modification Release This command was introduced. 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor 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 RP/0/RSP0/CPU0:router (config-if) # member vni 100-120 mcast-group 224.2.2.50 To use this command, you must be in a user group associated with a task group that incl	Command Modes NVE interface configuration Command History Release Modification Release This command was introduced. 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step		end_ip_address	The end multicast IP address from a range.	
Command History Release Modification Release This command was introduced. 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor 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 224.2.2.23 RP/0/RSP0/CPU0:router (config-if) # member vni 100-120 mcast-group 224.2.2.2 To use this command, you must be in a user group associated with a task group that incl	Command History Release Modification Release This command was introduced. 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step	Command Default	None		
Release 5.2.0 This command was introduced. 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perfor 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 RP/0/RSP0/CPU0:router(config-if)# member vni 100-120 mcast-group 224.2.2.50 RP/0/RSP0/CPU0:router(config-if)# member vni 100-120 mcast-group 224.2.2.50 To use this command, you must be in a user group associated with a task group that incl	Release This command was introduced. 5.2.0 5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step	Command Modes	NVE interface co	onfiguration	
5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform VXLAN or 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 RP/0/RSP0/CPU0:router(config-if)# member vni 100-120 mcast-group 224.2.2.50 To use this command, you must be in a user group associated with a task group that incl	5.2.0 Usage Guidelines To associate discontiguous VXLANs or VXLAN ranges with the NVE interface, perform this step	Command History	Release Mo	odification	
VXLAN or VXLAN range. For instance,RP/0/RSP0/CPU0:router(config-if)# member vni 10 mcast-group 224.2.2.10RP/0/RSP0/CPU0:router(config-if)# member vni 23 mcast-group 224.2.2.23RP/0/RSP0/CPU0:router(config-if)# member vni 50-59 mcast-group 224.2.2.50RP/0/RSP0/CPU0:router(config-if)# member vni 100-120 mcast-group 224.2.2.2To use this command, you must be in a user group associated with a task group that incl				his command was introduced.	
<pre>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 RP/0/RSP0/CPU0:router(config-if)# member vni 100-120 mcast-group 224.2.2.2 To use this command, you must be in a user group associated with a task group that incl</pre>		Usage Guidelines			
	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 224.2.2.50 224.2.2.5				
IDs. If the user group assignment is preventing you from using a command, contact you for assistance.	To use this command, you must be in a user group associated with a task group that includes approp IDs. If the user group assignment is preventing you from using a command, contact your AAA adm for assistance.		IDs. If the user gr		

Task ID Task ID Operation interface read,

	write
tunnel	read, write

member vni number

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 200.0.20.

```
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.

Syntax Description	vni	The mem	ber 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-de	omain confi	iguration
Command History	Release	Modif	fication
	Release 5.2.0	This c	command was introduced.
Usage Guidelines		e user group	d, you must be in a user group associated with a task group that includes appropriate tas p assignment is preventing you from using a command, contact your AAA administrate
Task ID	Task ID	Operation	
Task ID	Task ID interface		-

Example

The following example shows the VXLAN with VNI "5010" associated with the bridge domain "bd1".

```
RP/0/RSP0/CPU0:router(config)# 12vpn
RP/0/RSP0/CPU0:router(config-12vpn)# bridge group bg1
RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain bd1
RP/0/RSP0/CPU0:router(config-12vpn-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-enc	apsulation {vxlan}	
Syntax Description	vxlan Set	s the NVE interface as a VXLAN	J Terminal EndPoint (VTEP).
Command Default	The NVE in	terface provides VXLAN encaps	sulation.
Command Modes	NVE interfa	ce configuration	
Command History	Release	Modification	_
	Release 5.2.0	This command was introduced	_
Usage Guidelines		ser group assignment is preventir	group associated with a task group that includes appropriate task ng you from using a command, contact your AAA administrator
Task ID	Task ID Op	peration	
	interface rea	ad, rite	
		ad, rite	
	Example		

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.		
	Release 5.3.1	The show command output was enhanced to display VXLAN anycast gateway parameters.		
Usage Guidelines		ommand, you must be in a user group associated with a task group that includes appropriate task ser group assignment is preventing you from using a command, contact your AAA administrator e.		
Task ID	Task ID Op	eration		
	interface rea	ad		
	Example			
	This is the sagateway para	ample output for show interface nve command enhanced to display VXLAN anycast ameters.		
	<pre>RP/0/RSP0/CPU0:router(config)# show interface nvel00 detail Interface: nvel00 State: Up Encapsulation: VxLAN Source Interface: Loopback1 (primary: 1.1.1.1) Source Interface State: Up NVE Flags: 0x1, Admin State: Up, Interface Handle 0xba0 UDP Port: 4789 Anycast Source Interface: Loopback100 (primary: 100.1.1.1) Mcast Sync Group: 224.10.10.1 Mcast Flags: 0x1</pre>			
		ng shows an example output of the show interface nve command.		
	RP/0/RSP0/0 Interface:	CPU0:router(config)# show interface nve nvel detail nvel, State:up, encapsulation:VXLAN erface: Lo1 (primary:1.1.1.1, 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 j	peers [{interface nve nve-id	r ni vni-id}]	
Syntax Description	interface nve <i>nve-id</i> Displays NVE peers of the specified NVE interface.			
	vni vni-id	Displays NVE peers of	f the specified VNIs.	
Command Default	None			
Command Modes	EXEC			
Command History	Release	Modification		
	Release 5.2.0	This command was introduced.		
Usage Guidelines		arns about NVE peers through dat E peers only after VXLAN traffic		how nve peers command output
		ommand, you must be in a user gr ser group assignment is preventing e.	-	
Task ID	Task Ope ID	ration		
	tunnel read	d		

Example

I

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	1.1.1.2	1000	10h
nve2	1.1.1.3	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	detail			Displays more detailed output.
	interface n	ve nve-id			Displays details for the specific NVE interface.
Command Default	None				
Command Modes	EXEC				
Command History	Release	Modification	n		
	Release 5.2.0	This comma	nd was introdu	ced.	
Usage Guidelines	$\frac{5.2.0}{\text{To use this c}}$	ommand, you r ser group assign	must be in a us	er group associate	d with a task group that includes appropriate tas ing a command, contact your AAA administrate
Usage Guidelines Task ID	5.2.0 To use this c IDs. If the us for assistanc	ommand, you r ser group assign	must be in a us	er group associate	
	5.2.0 To use this c IDs. If the us for assistanc Task Ope	ommand, you r ser group assign e. eration	must be in a us	er group associate	
	5.2.0 To use this c IDs. If the us for assistanc Task Ope ID	ommand, you r ser group assign e. eration	must be in a us	er group associate	
	5.2.0 To use this c IDs. If the us for assistanc Task Ope ID tunnel read Example	ommand, you r ser group assign e. eration d	must be in a us nment is preve	er group associate	ing a command, contact your AAA administrate

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-inte	erface loopback interface-id			
Syntax Description	loopback Specifies a loopback interface as providing IP address for the NVE interface.				
	interface-id	<i>d</i> Specifies the loopback interface ID. It can take values from 0 to 65535.			
Command Default	None				
Command Modes	NVE interfa	ace configuration			
Command History	Release	Modification			
	Release 5.2.0	This command was introduced.			
Usage Guidelines		command, you must be in a user group associated with a task group that includes appropriate group assignment is preventing you from using a command, contact your AAA adm ce.			
Task ID	Task ID 0	peration			
		ead, vrite			
	interface re w	ead, vrite			
	Example				

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
```