

Point-to-Point Layer 2 Services Commands

This section describes the commands used to configure point-to-point services for Layer 2 VPNs.

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

For detailed information about concepts and configuration, see the Configure Point-to-Point Layer 2 Services chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series RoutersL2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series RoutersL2VPN and Ethernet Services Configuration Guide for Cisco NCS 560 Series Routers*

.

- interface (p2p), on page 3
- decoupled-mode, on page 5
- dynamic-arp-inspection, on page 6
- hw-module profile load-balance algorithm, on page 8
- hw-module profile l2pt-extended-protocols-enable, on page 11
- hw-module storm-control-combine-policer-bw, on page 12
- hw-module profile storm-control-policer, on page 13
- ip-source-guard, on page 16
- l2vpn, on page 17
- mac limit notification, on page 18
- mac limit threshold, on page 19
- mac secure, on page 20
- mac withdraw, on page 23
- p2p, on page 24
- pw-class (L2VPN), on page 25
- pw-class encapsulation mpls, on page 27
- show ethernet mac-allocation, on page 30
- show l2vpn, on page 31
- show l2vpn collaborators, on page 33
- show l2vpn bridge-domain (VPLS), on page 35
- show l2vpn database, on page 39
- show l2vpn forwarding, on page 42
- show l2vpn forwarding message counters, on page 47
- show l2vpn index, on page 52
- show l2vpn protection main-interface, on page 54
- show l2vpn resource, on page 57
- show l2vpn trace, on page 58
- show l2vpn xconnect, on page 61
- show l2vpn pw-class, on page 64
- storm-control , on page 66
- vlan-switch vsp, on page 68
- xconnect group, on page 69

interface (p2p)

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

interface *type interface-path-id* **l2transport**
no interface *type interface-path-id* **l2transport**

Syntax Description

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

Command Default

None

Command Modes

p2p configuration sub-mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
Router# configure
Router(config)# interface TenGigE 0/0/0/10.20 l2transport
Router(config-subif)# encapsulation dot1ad 3000
Router(config-subif)# commit
Router(config-subif)#
```

Related Commands

Command	Description
l2transport (Ethernet)	Enables Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode.
encapsulation dot1ad	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.

decoupled-mode

To configure decoupled AC-PW state mode, use the **decoupled-mode** command in L2VPN xconnect p2p configuration submode.

decoupled-mode

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

L2VPN xconnect p2p

Command History

Release	Modification
Release 25.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows a point-to-point cross-connect configuration with decoupled-mode enabled.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group 1
Router(config-l2vpn-xc)# p2p 1
Router(config-l2vpn-xc-p2p)# decoupled-mode
Router(config-l2vpn-xc-p2p)# commit
```

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*}}

Syntax Description

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

Command Default

Dynamic ARP inspection is disabled.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

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

```
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection logging
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# dynamic-arp-inspection address-validation
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-dai)#
```

hw-module profile load-balance algorithm

To enable the load-balancing mode for PPPoE traffic in the router, use the **hw-module profile load-balance algorithm** command in the Global Configuration mode.

hw-module profile load-balance algorithm { **L3-only** | **PPPoE** | **gtp** | **gtp-mpls** | **inner-l2-field** | **ip-tunnel** | **layer2** | **mpls-lsr-ler** | **mpls-lsr-ler-optimized** | **mpls-safe-speculative-parsing** | **fat-based-hash** }

Syntax Description

ip-tunnel	Allows the hashing algorithm to use the outer IPv4 GRE header even while doing an IP tunnel decapsulation.
layer2	Allows the hashing algorithm to use the inner IP header information while doing layer 2 forwarding with inner payload as MPLS.
gtp	Allows hashing based on the tunnel id in GTP-U packets.
gtp-mpls	Allows hashing based on the tunnel id in GTP-U packets intead of Layer 4 packets when underlay network is MPLS.
mpls-safe-speculative-parsing	Allows hashing based on the first nibble of the MAC DA address.
pppoe	Allows hashing based on inner IPv4 or IPv6 headers for PPPoE packets to perform the traffic load-balancing. We recommend enabling this hashing on head and tail nodes.
L3-Only	Allows hashing for L3 header only. We recommend enabling this hashing when majority of traffic is fragmented.
mpls-lsr-ler	Allows hashing in Label Edge Router (LER) and Label Switched Routers (LSRs) with MPLS traffic. This profile is recommended to be used when the following traffic flows are prominent: • IPv4 pop and lookup flows (EthoMPLS2/3oIPv4oL4) with L4 as TCP or UDP • IPv6 pop and lookup flows (EthoMPLS2/3oIPv6oXX) with L4 as TCP or UDP
mpls-lsr-ler-optimized	Allows optimized hashing in LER and LSR with MPLS IPv6 traffic. This profile is recommended to be used when the following traffic flows are prominent: • 4 Label IPv6 flows (EthoMPLS4/6oIPv6) • IPv6 pop and lookup flows (EthoMPLS2/3oIPv6oXX) with L4 as non-TCP/UDP (for example, no next header, GRE)
inner-L2-field	Allows the hashing algorithm to use the inner ethernet fields of the source MAC and destination MAC addresses.

fat-based-hash	Allows fat label based load-balancing on L2VPN decapsulation node or egress PE.

Command Default

The load-balancing mode is disabled by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 24.4.1	The fat-based-hash keyword is introduced.
Release 7.4.1	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.

Without control-word, L2VPN traffic is considered to be IPv4 or IPv6 traffic depending on the presence of nibble 4 or nibble 6 in the payload after the last label in the traffic. The matching offset fields are considered for load-balancing hash calculation. This may cause hashing of a single flow to different links resulting in decrease of end user throughput.

While adding or removing these commands, you must reload the router.

- **hw-module profile load-balance algorithm ip-tunnel**
- **hw-module profile load-balance algorithm PPPoE**
- **hw-module profile load-balance algorithm fat-based-hash**

The **hw-module profile segment-routing srv6** is mutually exclusive with **hw-module profile load-balance algorithm PPPoE** and **hw-module profile load-balance algorithm ip-tunnel** commands.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable the load-balancing mode for PPPoE traffic on the router at the encapsulation node:

```
Router# configure
Router(config)# hw-module profile load-balance algorithm PPPoE
Router(config)# exit
Router# reload
```

The following example shows how to enable fat label-based load balancing on L2VPN decapsulation node or egress PE:

```
Router# configure
Router(config)# hw-module profile load-balance algorithm fat-based-hash
```

```
Router(config)# exit
Router# reload
```

hw-module profile l2pt-extended-protocols-enable

To configure extended Layer 2 protocol tunneling on an Ethernet interface, use the **hw-module profile l2pt-extended-protocols-enable** command in Layer 2 transport configuration mode. To disable a Layer 2 protocol tunneling configuration, use the **no** form of this command.

hw-module profile l2pt-extended-protocols-enable
no hw-module profile l2pt-extended-protocols-enable

Syntax Description

l2pt-extended-protocols-enable	Enables L2PT for the interface. Along with exisiting tunneling protocols like CDP, PVRST, STP, VTP, the following extended protocols are supported for tunneling by using the **hw-module profile l2pt-extended-protocols-enable** command: • Link Layer Discovery Protocol (LLDP) • Link Aggregation Control Protocol (LACP) • Operation, Administration, Management (OAM) • Ethernet Local Management Interface (ELMI) • EtherChannel Port Aggregation Protocol (PAgP) • Unidirectional Link Detection (UDLD) • Multiple MAC Registration Protocol (MMRP) • Multiple VLAN Registration Protocol (MVRP) • 802.1X protocol

Syntax Description

This command has no arguments or keywords.

Command Default

The Layer 2 extended protocols are disabled by default.

Command Modes

Layer 2 transport configuration mode

Command History

Release	Modification
Release 7.9.1	This command was introduced for NCS 540 series routers.

Examples

The following example shows how to configure an Ethernet interface to tunnel in the ingress direction with extended Layer 2 protocol tunneling:

```
Router# configure
Router(config)# hw-module profile l2pt-extended-protocols-enable
Router(config)# exit
Router# reload
```

hw-module storm-control-combine-policer-bw

To increase the storm control policer scale per NPU core, use the **hw-module storm-control-combine-policer-bw** command in the global configuration mode. To disable storm control, use the **no** form of this command.

hw-module storm-control-combine-policer-bw enable

Command Default

Storm control combine is disabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 7.4.1	This command was introduced for Cisco NC57 line cards.
Release 7.8.1	This command was modified to support storm control configuration per subinterface.

Usage Guidelines

You must manually reload the router to activate the **hw-module storm-control-combine-policer-bw enable** command.

Examples

The following example activates the combined policer mode:

```
Router# configure
Router#(config)# hw-module storm-control-combine-policer-bw enable
Router# commit
```

The following example shows storm control configuration per subinterface:

```
Router# configure
Router(config)# hw-module storm-control-combine-policer-bw enable
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# interface HundredGigE0/0/0/1.10
Router(config-l2vpn-bg-bd-ac)# storm-control unknown-unicast pps 500
Router(config-l2vpn-bg-bd-ac)# storm-control multicast pps 2000
Router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 1000
Router(config-l2vpn-bg-bd-ac)# commit
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# interface HundredGigE0/0/0/1.20
Router(config-l2vpn-bg-bd-ac)# storm-control unknown-unicast pps 200
Router(config-l2vpn-bg-bd-ac)# storm-control multicast pps 1000
Router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 2000
Router(config-l2vpn-bg-bd-ac)# commit
Router(config-l2vpn-bg-bd-ac)# exit
```

hw-module profile storm-control-policer

To enable traffic policing using the storm control policer profile and track the storm control policer allocation on the router, use the **hw-module profile storm-control-policer enable** command in the global configuration mode. To disable storm control, use the **no** form of this command.

hw-module profile storm-control-policer enable

Command Default

Storm control policer profile is disabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 25.1.1	This command was introduced for Cisco NCS 540 router.

Usage Guidelines

You must manually reload the router to activate the **hw-module profile storm-control-policer enable** command.

Examples

The following example activates the combined policer mode:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#hw-module profile storm-control-policer enable
RP/0/RP0/CPU0:router(config)# commit
In order to activate this storm-control-policer, you must manually reload the chassis.
Please note that after enabling storm controller, tetx-srv6loc will not have a dedicated
engine
After reload the engine 0 is allocated to sc_policer
```

The following example shows that storm control policer is allocated to engine 0 with the total counter entries size for engine 0 of 4k:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#hw-module profile storm-control-policer enable
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# exit
RP/0/RP0/CPU0:ios#show controllers npu resources stats internal instance all location all
Mon Feb 17 18:16:03.132 UTC
HW Stats Information For Location: 0/RP0/CPU0
System information for NPU 0:
Counter Processor Configuration Profile: Default
================================================================================================
Assigned Counter Engine Resource Information
================================================================================================
Feature                Eng    State   Eng   Total Counter    Core-0 Entries  Core-1 Entries

                        Id             Size    Entries          InUse           InUse

================================================================================================
trap-aclpolicer         7     In use   4K     2048            147             147
```

lpts-pbr	15	In use	8K	4096	60	60
aclrx-mcrouterx	4	Free	4K	4096	0	0
aclrx-mcrouterx	5	Free	4K	4096	0	0
acltx	6	Free	4K	4096	0	0
qos rx	22	Free	16K	8192	0	0
qos rx	23	Free	16K	8192	0	0
qos rx	24	Free	16K	8192	0	0
qos rx	25	Free	16K	8192	0	0
qos rx	26	Free	16K	8192	0	0
qos rx	27	Free	16K	8192	0	0
voq	16	In use	16K	8192	35	35
voq	17	Free	16K	8192	0	0
voq	18	Free	16K	8192	0	0
voq	19	Free	16K	8192	0	0
voq	20	Free	16K	8192	0	0
voq	21	Free	16K	8192	0	0
l3rx	12	In use	8K	8192	3	3
l3rx	13	Free	8K	8192	0	0
l3rx	14	Free	8K	8192	0	0
mplsrx-l3rxbgppa	3	Free	4K	4096	0	0
l2rx	9	In use	8K	8192	0	2
l3tx	1	Free	4K	4096	0	0
l3tx2	2	In use	4K	2048	11	11
l2tx-mctx	10	In use	8K	8192	0	2
l2tx-mctx	11	Free	8K	8192	0	0
tetx-srv6loc	8	Free	8K	8192	0	0
POLICER1 (CHILD)	28	Reserved	16K	16384	0	0
POLICER1 (CHILD)	29	Reserved	16K	16384	0	0
POLICER1 (CHILD)	30	Reserved	16K	16384	0	0
POLICER1 (CHILD)	31	Reserved	16K	16384	0	0
POLICER2 (PARENT)	32	Reserved	16K	16384	0	0
Storm Control Policer	**0**	**Reserved**	**4K**	**4096**	0	0

```
================================================================================
Note: Free and Unassigned Counter engines can be reassigned to other features
================================================================================
```

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

Syntax Description

logging	(Optional) Enables logging.

Command Default

IP Source Guard is disabled.

Command Modes

l2vpn bridge group bridge domain configuration

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# ip-source-guard
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ipsg)#
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group b1
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain bar
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# ip-source-guard logging
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ipsg)#
```

l2vpn

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

l2vpn
no l2vpn

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enter L2VPN configuration mode:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)#
```

mac limit notification

To generate syslog messages and SNMP trap notifications, use the **mac limit notification** command in the L2VPN BD configuration mode.

mac limit notification [**both** | **none** | **trap**]

Syntax Description

both	Generates syslog message and SNMP trap messages.
none	No notifications are generated.
trap	Generates only SNMP trap messahes

Command Default

None.

Command Modes

L2VPN bridge-domain configuration mode

Command History

Release	Modification
Release 6.1.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to generate syslogs and SNMP trap messages:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 555
Router(config-l2vpn-bg)# bridge-domian 666
Router(config-l2vpn-bg-bd)# mac limit notification both
Router(config-l2vpn-bg-bd)#commit
```

mac limit threshold

To configure MAC address limit threshold value, use the **mac limit threshold** command in the L2VPN configuration mode.

mac limit threshold *value*

Syntax Description

value	Specifies MAC limit threshold value. The valid range is 0 - 100 %.

Command Default

75%.

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 6.1.0	This command was introduced.

Usage Guidelines

MAC address limit action applies only when the number of local MAC addresses exceeds the configured limit. The software unlearns the MAC addresses until it reaches the configured MAC limit threshold value. Later, the router restarts learning new MAC addresses. In the event when the MAC limit threshold is not configured, the default threshold is 75% of the configured MAC address limit.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to configure MAC limit threshold of 80%:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# mac limit threshold 80
Router(config-l2vpn)#commit
```

mac secure

To configure MAC security at a port and to set the action that is to be taken when security is violated, use the **mac secure** command in the L2VPN bridge-group, bridge-domain configuration mode and in the EVPN configuration mode.

To configure MAC security in the L2VPN bridge-group, bridge-domain configuration mode use:

mac secure { **action** [**none** | **shutdown**] | **logging** | **threshold** | **shutdown-recovery-timeout** *timer-value* }

Syntax Description

action	(Optional) Indicates the action to be taken when security is violated.
none	Forwards the violating packet and allows the MAC address to be relearned.
shutdown	Shuts down the violating bridge port.
logging	(Optional) Enables logging.
threshold	Specify the maximum number of MAC address moves allowed within a specified time interval. By default, the threshold allows five MAC moves within a 180-second move interval if not explicitly configured. When the number of MAC moves exceeds the configured threshold within the move interval, the system marks the MAC address entry as duplicate and shuts down the corresponding port to prevent potential Layer 2 network loops. For more information, see MAC Loop Prevention section in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.
shutdown-recovery-timeout *timer-value*	Sets the Recovery timer to revert shutdown action automatically after the timer expires. Recovery timer value can be set in the range of 10 to 3600 seconds.

To configure MAC security in the EVPN configuration mode use:

mac secure [**freeze-time** *freeze-time* | **move-count** *move-count* | **move-interval** *move-interval* | **retry-count** *retry-count* | | **reset-freeze-count-interval** *interval*] **disable**

Syntax Description

freeze-time *freeze-time*	Length of time to lock the MAC address after it has been detected as duplicate. Default is 30 seconds.
move-count *move-count*	Number of moves to occur witin the specified **move-interval** before freezing the MAC address. Default is 5.
move-interval *move-interval*	Interval to watch for subsequent MAC moves before freezing the MAC address. Default is 180 seconds.
retry-count *retry-count*	Number of times to unfreeze a MAC address before freezing it permanently. Default is three times.

reset-freeze-count-interval *interval*	Interval after which the count of duplicate detection events is reset. Default is 24 hours. The range is from is 1 hour to 48 hours.
disable	Disable duplicate detection of MAC address.

Command Default

None

Command Modes

L2VPN bridge-group, bridge-domain configuration

EVPN configuration

Command History

Release	Modification
Release 7.5.1	This command was introduced.

Usage Guidelines

MAC secure is not supported on physical ACs, bundle ACs, and PWs.

In EVPN, MAC secure supports only loop detection with the following options:

```
mac secure [ freeze-time freeze-time | move-count move-count | move-interval move-interval
 | retry-count retry-count | reset-freeze-count-interval interval ] disable
```

Task ID

Task ID	Operations
l2vpn	Read, write

Examples

This example shows how to enable MAC security in the L2VPN bridge-group, bridge-domain configuration mode.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge-group BG1
Router(config-l2vpn-bg)# bridge-domain BD1
Router(config-l2vpn-bg-bd)# mac secure
Router(config-l2vpn-bg-bd-mac-sec)# action shutdown
Router(config-l2vpn-bg-bd-mac-sec)# threshold
Router(config-l2vpn-bg-bd-mac-sec)# shutdown-recovery-timeout 300
Router(config-l2vpn-bg-bd-mac-sec)# exit
Router(config-l2vpn-bg-bd)# interface GigabitEthernet0/2/0/0.1
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# interface GigabitEthernet0/2/0/0.2
Router(config-l2vpn-bg-bd-ac)# commit
```

Examples

This example shows how to enable MAC security in the EVPN configuration mode.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# mac secure
Router(config-evpn-mac-secure)# move-count 7
```

```
Router(config-evpn-mac-secure)# move-interval 30
Router(config-evpn-mac-secure)# commit
```

mac withdraw

To enable MAC address withdrawal for a specified bridge domain, use the **mac withdraw** command in L2VPN configuration mode.

mac withdraw [**disable** | **optimize** | **state-down**]

Syntax Description

disable	Disables MAC address withdrawal.
optimize	Enables optimization of MAC address withdrawal when the bridge port goes down.
state-down	Sends MAC address withdrawal message when the bridge port goes down.

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

The following example shows how to disable MAC address withdrawal.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw disable
```

The following example shows how to configure MAC address withdrawal when the bridge port goes down.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw state-down
```

The following example shows how to configure optimization of MAC address withdrawal when the bridge port goes down.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw optimize
```

p2p

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

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

Syntax Description

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

Command Default

None

Command Modes

L2VPN xconnect

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows a point-to-point cross-connect configuration:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p XCON1_P2P3
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/0
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/8
Router(config-l2vpn-xc-p2p)# commit
```

pw-class (L2VPN)

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

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

Syntax Description

class-name	Pseudowire class name.

Command Default

None

Command Modes

L2VPN configuration sub-mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group l1vpn
Router(config-l2vpn-xc)# p2p rtrA_to_rtrB
Router(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
Router(config-l2vpn-xc-p2p-pw)# pw-class kanata01
Router(config-l2vpn-xc-p2p-pw)# encapsulation mpls
Router(config-l2vpn-xc-p2p-pw)# exit
Router(config-l2vpn-xc-p2p)# exit
Router(config-l2vpn)# commit
```

Related Commands

Command	Description
interface (p2p), on page 3	Configures an attachment circuit.

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
show l2vpn, on page 31	Displays L2VPN information
show l2vpn xconnect, on page 61	Displays brief information on configured cross-connects.
show l2vpn pw-class, on page 64	Displays L2VPN pseudowire class information.

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

Syntax Description

class-name	Encapsulation class name.
control word	Disables control word for MPLS encapsulation. Disabled by default.
ipv4	Sets the local source IPv4 address.
load-balancing flow-label	Sets flow label-based load balancing.
preferred-path	Configures the preferred path tunnel settings.
protocol ldp	Configures LDP as the signaling protocol for this pseudowire class.
redundancy one-way	Configures one-way PW redundancy behavior in the Redundancy Group.
sequencing	Configures sequencing on receive or transmit.
tag-rewrite	Configures VLAN tag rewrite.

transport-mode	Configures transport mode to be Ethernet. The transport-mode VLAN is not suppported. **Note** The transport-mode VLAN is not suppported for VPWS. **Note** The system does not support transport-mode under pw-class for VPLS. The transport-mode configurartion is not supported under pw-class, and it is supported only under bridge domain for NCS 5500.
vccv none	Enables or disables the VCCV verification type.

Command Default None

Command Modes L2VPN pseudowire class configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples This example shows how to define MPLS pseudowire encapsulation:

```
Router# configure
Router(config)# l2vpn
```

```
Router(config-l2vpn)# pw-class kanata01
Router(config-l2vpn-pwc)# encapsulation mpls
```

Related Commands

Command	Description
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.

show ethernet mac-allocation

To display the number of dynamically allocated MAC addresses information, use the **show ethernet mac-allocation** command in the EXEC mode.

show ethernet mac-allocation [**client** | **clients** | **detail** | **error** | **server** | **statistics** | **summary** | **trace**]

Syntax Description

client	Shows MAC allocation client library trace data.
clients	Shows the MAC allocation on client information.
detail	Shows the detailed information of MAC allocation.
error	Shows error traces only.
server	Shows MAC allocation server trace data.
statistics	Shows the statistic details.
summary	Shows the summary information.
trace	Shows MAC allocation trace data.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced. Applicable to N540-28Z4C-SYS-A/D, N540X-16Z4G8Q2C-A/D, N540-12Z20G-SYS-A/D, and N540X-12Z16G-SYS-A/D variants.

Example

The following example displays summary of MAC allocation, **show ethernet mac-allocation summary** command.

```
Router# show ethernet  mac-allocation summary

Mon Jun 14 04:11:41.168 UTC
Minimum pool size:      3072
Pool increment:         1
Maximum free addresses: Unlimited
Configured pool size:   0 (0 free)
Dynamic pool size:      3072 (3061 free)
Total pool size:        3072 (3061 free)
Number of clients:      2
```

show l2vpn

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

show l2vpn

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

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

```
Router# show l2vpn

Mon Oct 12 14:14:48.869 UTC
HA role     : Active
ISSU role   : Primary
Process FSM : PrimaryActive
---------------------------
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
```

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.

Command	Description
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.

show l2vpn collaborators

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

show l2vpn collaborators

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
Router# show l2vpn collaborators
Mon Oct 12 14:14:57.373 UTC

L2VPN Collaborator stats:
Name                 State       Up Cnts      Down Cnts
-------------------  ----------  -----------  -----------
                 LSD          Up            1            0
```

This table describes the significant fields shown in the display.

Table 1: show l2vpn collaborators Field Descriptions

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

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

Related Commands

Command	Description
show l2vpn, on page 31	Displays L2VPN information

show l2vpn bridge-domain (VPLS)

To display information for the bridge ports such as attachment circuits and pseudowires for the specific bridge domains, use the **show l2vpn bridge-domain** command in XR 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.
bd-name *bridge-domain-name*	(Optional) Displays filter information on the *bridge-domain-name*. The *bridge-domain-name* argument is used to name a bridge domain.
brief	(Optional) Displays brief information about the bridges.
detail	(Optional) Displays detailed information about the bridges. Also, displays the output for the Layer 2 VPN (L2VPN) to indicate whether or not the MAC withdrawal feature is enabled and the number of MAC withdrawal messages that are sent or received from the pseudowire.
group *bridge-domain-group-name*	(Optional) Displays filter information on the bridge-domain group name. The *bridge-domain-group-name* argument is used to name the bridge domain group.
hardware	(Optional) Displays hardware information.
interface *type interface-path-id*	(Optional) Displays the filter information for the interface on the bridge domain. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
neighbor *ip-address*	(Optional) Displays the bridge domains that contain the pseudowires to match the filter for the neighbor. The *ip-address* argument is used to specify IP address of the neighbor.
pw-id *value*	(Optional) Displays the filter for the pseudowire ID. The range is from 1 to 4294967295.
pbb	(Optional) Displays provider backbone bridge information.
summary	(Optional) Displays the summary information for the bridge domain.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification

Usage Guidelines

Use the **interface** keyword to display only the bridge domain that contains the specified interface as an attachment circuit. In the sample output, only the attachment circuit matches the filter that is displayed. No pseudowires are displayed.

When an SR policy is configured as the preferred path for a VPLS circuit, the traffic traverses through the SR policy path. The PW counters are updated with statistics about packets transmitted and received. When the SR policy configuration is deleted, the traffic session is still functional because the traffic transmission switches back to the normal LSP path between the PEs. There is no drop in the end-to-end traffic transmitted. However, the packet statistics counters are reset and start from zero. This is because, when the SR policy is deleted, the PW too gets deleted and the statistics information associated with the old PW is cleared. The counter restarts from zero when the new PW is created after the switch takes place.

Task ID

Task ID	Operations
l2vpn	read

Examples

This is the sample output for **show l2vpn bridge-domain** command.

```
RP/0/RP0/CPU0:router# show l2vpn bridge-domain bd-name evpn detail
Fri Dec 11 06:58:17.691 UTC
Legend: pp = Partially Programmed.
Bridge group: evpn-aa-irb-inter, bridge-domain: evpn, id: 1797, state: up, ShgId: 0, MSTi:
 0
  Coupled state: disabled
  VINE state: EVPN-IRB
  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: 64000, Action: none, Notification: syslog
  MAC limit reached: no, threshold: 99%
  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
  DHCPv4 Snooping profile: none
  IGMP Snooping: disabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
  Storm Control: disabled
  Bridge MTU: 1500
  MIB cvplsConfigIndex: 1798
  Filter MAC addresses:
  P2MP PW: disabled
  Multicast Source: Not Set
  Create time: 11/12/2020 02:02:56 (04:55:20 ago)
  No status change since creation
  ACs: 2 (2 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of EVPNs:
    EVPN, state: up
```

```
      evi: 2001
      XC ID 0x800006a7
     Statistics:
       packets: received 0 (unicast 0), sent 0
       bytes: received 0 (unicast 0), sent 0
       MAC move: 0
  List of ACs:
    AC: BVI10001, state is up
      Type Routed-Interface
      MTU 2000; XC ID 0x80000fa3; interworking none
      BVI MAC address:
        0088.0088.0088
      Split Horizon Group: Access
      PD System Data: AF-LIF-IPv4: 0x00000000  AF-LIF-IPv6: 0x00000000 FRR-LIF: 0x00000000

    AC: Bundle-Ether30001.2001, state is up
      Type VLAN; Num Ranges: 1
      Outer Tag: 3001
      Rewrite Tags: []
      VLAN ranges: [2001, 2001]
      MTU 1500; XC ID 0xa00005e0; interworking none; MSTi 1
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 64000, Action: none, Notification: syslog
      MAC limit reached: no, threshold: 99%
      MAC port down flush: enabled
      MAC Secure: disabled, Logging: disabled
      Split Horizon Group: none
      E-Tree: Root
      Dynamic ARP Inspection: disabled, Logging: disabled
      IP Source Guard: disabled, Logging: disabled
      DHCPv4 Snooping: disabled
      DHCPv4 Snooping profile: none
      IGMP Snooping: disabled
      IGMP Snooping profile: none
      MLD Snooping profile: none
      Storm Control: bridge-domain policer
      Static MAC addresses:
      Statistics:
        packets: received 404672709 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 0
        bytes: received 30835628366 (multicast 0, broadcast 0, unknown unicast 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
      Dynamic ARP inspection drop counters:
        packets: 0, bytes: 0
      IP source guard drop counters:
        packets: 0, bytes: 0
      PD System Data: AF-LIF-IPv4: 0x00018919  AF-LIF-IPv6: 0x0001891a FRR-LIF: 0x00000000

  List of Access PWs:
  List of VFIs:
  List of Access VFIs:
```

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.

Command	Description
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information

show l2vpn database

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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:

```
Router# show l2vpn database ac

Mon Oct 12 14:15:47.731 UTC
Bundle-Ether1:
      Other-Segment MTU: 0
      Other-Segment status flags: 0x3
      Signaled capability valid: Yes
      Signaled capability flags: 0x360018
      Configured capability flags: 0x0
      XCID: 0xa0000001
      PSN Type: Undefined
      ETH data:
          Xconnect tags: 0
          Vlan rewrite tag: 0
    AC defn:
        ac-ifname: Bundle-Ether1
        capabilities: 0x00368079
        extra-capabilities: 0x00000000
        parent-ifh: 0x00000000
        ac-type: 0x04
        interworking: 0x00
    AC info:
        seg-status-flags: 0x00000003
        segment mtu/l2-mtu: 1500/1514
```

```
TenGigE0/0/0/0.1:
      Other-Segment MTU: 0
      Other-Segment status flags: 0x3
      Signaled capability valid: Yes
      Signaled capability flags: 0x360018
      Configured capability flags: 0x0
      XCID: 0xea
      PSN Type: Undefined
      ETH data:
          Xconnect tags: 0
          Vlan rewrite tag: 0
    AC defn:
        ac-ifname: TenGigE0_0_0_0.1
        capabilities: 0x00368079
        extra-capabilities: 0x00000000
        parent-ifh: 0x08000018
        ac-type: 0x15
        interworking: 0x00
    AC info:
        seg-status-flags: 0x00000003
        segment mtu/l2-mtu: 1504/1518
```

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

```
Router# show l2vpn database node
Mon Oct 12 14:16:30.540 UTC
Node ID: 0x1000 (0/RP0/CPU0)
   MA: vlan_ma      inited:1, flags:0x 2, circuits:3744
     AC event trace history [Total events: 4]
     ----------------------------------------
     Time                Event                          Num Rcvd    Num Sent
     ====                =====                          ========    ========
     10/12/2015 12:46:00 Process joined                 0           0
     10/12/2015 12:46:00 Process init success           0           0
     10/12/2015 12:46:00 Replay start rcvd              0           0
     10/12/2015 12:46:00 Replay end rcvd                0           0

   MA: ether_ma     inited:1, flags:0x 2, circuits:2
     AC event trace history [Total events: 4]
     ----------------------------------------
     Time                Event                          Num Rcvd    Num Sent
     ====                =====                          ========    ========
     10/12/2015 12:41:19 Process joined                 0           0
     10/12/2015 12:41:19 Process init success           0           0
     10/12/2015 12:41:19 Replay start rcvd              0           0
     10/12/2015 12:41:19 Replay end rcvd                0           0

   MA: atm_ma       inited:0, flags:0x 0, circuits:0
   MA: hdlc_ma      inited:0, flags:0x 0, circuits:0
   MA: fr_ma        inited:0, flags:0x 0, circuits:0
   MA: ppp_ma       inited:0, flags:0x 0, circuits:0
   MA: cem_ma       inited:0, flags:0x 0, circuits:0
   MA: vif_ma       inited:0, flags:0x 0, circuits:0
   MA: pwhe_ma      inited:0, flags:0x 0, circuits:0
   MA: nve_mgr      inited:0, flags:0x 0, circuits:0
   MA: mstp         inited:0, flags:0x 0, circuits:0
   MA: span         inited:0, flags:0x 0, circuits:0
   MA: erp          inited:0, flags:0x 0, circuits:0
   MA: erp_test     inited:0, flags:0x 0, circuits:0
```

```
MA: mstp_test    inited:0, flags:0x 0, circuits:0
MA: evpn         inited:0, flags:0x 0, circuits:0
```

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information

show l2vpn forwarding

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

show l2vpn forwarding { **counter** | **debug** | **detail** | **hardware** | **interface** | **bridge-domain** [*bridge-domain-name*] | **mac-address** | **location** [*node-id*] | **private** }

Syntax Description

counter	Displays the cross-connect counters.
debug	Displays debug information.
detail	Displays detailed information from the layer2_fib manager.
hardware	Displays hardware-related layer2_fib manager information.
interface	Displays the match AC subinterface.
bridge-domain *bridge-domain-name*	(Optional) Displays filtered information on the *bridge-domain-name*. Use the *bridge-domain-name* argument to specify a name for a bridge domain.
mac-address	(Optional) Displays information about MAC addresses in a specific bridge domain within a L2VPN forwarding context.
location *node-id*	Displays layer2_fib manager information for the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.
private	Output includes private information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
Router# show l2vpn forwarding location 0/RP0/CPU0
Mon Oct 12 14:19:11.771 UTC
Segment 1                         Segment 2                         State
--------------------------------- --------------------------------- ------
Te0/0/0/0.234                     ac Te0/0/0/26.234                 UP
Te0/0/0/0.233                     ac Te0/0/0/26.233                 UP
Te0/0/0/0.232                     ac Te0/0/0/26.232                 UP
Te0/0/0/0.231                     ac Te0/0/0/26.231                 UP
Te0/0/0/0.230                     ac Te0/0/0/26.230                 UP
```

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

```
Router# show l2vpn forwarding counter location 0/RP0/CPU0

Mon Oct 12 14:18:01.194 UTC
Legend: ST = State, DN = Down

Segment 1                         Segment 2                         ST Byte
                                                                       Switched
--------------------------------- --------------------------------- -- ---------
Te0/0/0/0.234                     ac Te0/0/0/26.234                 UP 15098997504
Te0/0/0/0.233                     ac Te0/0/0/26.233                 UP 15098997568
Te0/0/0/0.232                     ac Te0/0/0/26.232                 UP 15098997504
Te0/0/0/0.231                     ac Te0/0/0/26.231                 UP 15098997568
Te0/0/0/0.230                     ac Te0/0/0/26.230                 UP 15098997568
```

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

```
Router# show l2vpn forwarding summary location 0/RP0/CPU0
 Mon Oct 12 14:18:25.838 UTC
 To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Major version num:1, minor version num:0
Shared memory timestamp:0xa41120d180
Global configuration:
Number of forwarding xconnect entries:1873
  Up:1873  Down:0
  AC-PW(atom):0 AC-PW(l2tpv2):0 AC-PW(l2tpv3):0
  AC-PW(l2tpv3-ipv6):0
  AC-AC:1873  AC-BP:0 (PWHE AC-BP:0) AC-Unknown:0
  PW-BP:0  PW-Unknown:0
  PBB-BP:0  PBB-Unknown:0
  EVPN-BP:0  EVPN-Unknown:0
  VNI-BP:0 VNI-Unknown:0
  Monitor-Session-PW:0  Monitor-Session-Unknown:0
Number of xconnects down due to:
  AIB:0  L2VPN:0  L3FIB:0  VPDN:0
Number of xconnect updates dropped due to:
  Invalid XID: 0 VPWS PW, 0 VPLS PW, 0 Virtual-AC, 0 PBB,
 0 EVPN
 0 VNI
Exceeded max allowed: 0 VPLS PW, 0 Bundle-AC
Number of p2p xconnects: 1873
Number of bridge-port xconnects: 0
Number of nexthops:0
Number of bridge-domains: 0
  0 with routed interface
  0 with PBB-EVPN enabled
  0 with 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 PWHE Main-port entries: 0
Number of EVPN Multicast Replication lists: 0 (0 default)
```

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

```
Router# show l2vpn forwarding detail location 0/RP0/CPU0

Mon Oct 12 14:18:47.187 UTC
Local interface: TenGigE0/0/0/0.234, Xconnect id: 0x1, Status: up
  Segment 1
    AC, TenGigE0/0/0/0.234, status: Bound
    Statistics:
      packets: received 238878391, sent 313445
      bytes: received 15288217024, sent 20060480
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0
  Segment 2
    AC, TenGigE0/0/0/26.234, status: Bound

Local interface: TenGigE0/0/0/0.233, Xconnect id: 0x2, Status: up
  Segment 1
    AC, TenGigE0/0/0/0.233, status: Bound
    Statistics:
      packets: received 238878392, sent 313616
      bytes: received 15288217088, sent 20071424
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0
  Segment 2
    AC, TenGigE0/0/0/26.233, status: Bound

Local interface: TenGigE0/0/0/0.232, Xconnect id: 0x3, Status: up
 Segment 1
    AC, TenGigE0/0/0/0.232, status: Bound
    Statistics:
      packets: received 238878391, sent 313476
      bytes: received 15288217024, sent 20062464
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0
  Segment 2
    AC, TenGigE0/0/0/26.232, status: Bound
```

Examples

The **show l2vpn forwarding bridge-domain** [*bridge-domain-name*] mac-address location [*node-id*] command displays MAC addresses from a specified location in the chassis.

Note that the **show l2vpn forwarding bridge-domain** [*bridge-domain-name*] mac-address location [*node-id*] command output may vary depending on the Cisco IOS XR software version. The example outputs given here are applicable for Release 7.10.x and later.

The show command displays MAC addresses learned from the local line card 0/2/CPU0 in the chassis.

```
Router#show l2vpn forwarding bridge-domain bg:bd mac-address location 0/2/CPU0
Fri Nov 29 09:29:56.034 UTC
 To Resynchronize MAC table from the Network Processors, use the command...
```

```
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on LC learned Resync Age/Last Change Mapped
to
-------------- ------- ---------                ---------- --------------         -------
0010.7777.7777 dynamic BE100.1                     N/A        29 Nov 09:29:56        N/A

0010.7777.7778 dynamic BE100.1                     N/A        29 Nov 09:29:56        N/A

0010.7777.7779 dynamic BE100.1                     N/A        29 Nov 09:29:56        N/A
```

The show command displays MAC addresses learned from the remote line card 0/1/CPU0 in the chassis.

```
Router#show l2vpn forwarding bridge-domain bg:bd mac-address location 0/1/CPU0
Fri Nov 29 09:37:16.884 UTC
 To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on LC learned Resync Age/Last Change Mapped
to
-------------- ------- ---------- ----------    ------------ --------------       --------
0010.7777.7777 dynamic BE100.1                     N/A        Remotely Aged          N/A

0010.7777.7778 dynamic BE100.1                     N/A        Remotely Aged          N/A

0010.7777.7779 dynamic BE100.1                     N/A        Remotely Aged          N/A
```

The show command displays MAC addresses learned from a remote EVPN peer multihoming node.

```
Router#show l2vpn forwarding bridge-domain bg:bd mac-address location 0/0/CPU0
Fri Nov 29 09:45:32.063 UTC
 To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on LC learned Resync Age/Last Change Mapped
to
-------------- ------- ----------               ---------------------- ---------- ----
0010.7777.7777 dynamic BE100.1                     N/A        Remotely Aged          N/A

0010.7777.7778 dynamic BE100.1                     N/A        Remotely Aged          N/A

0010.7777.7779 dynamic BE100.1                     N/A        Remotely Aged          N/A
```

The show command displays MAC addresses learned from a remote EVPN node.

```
Router#show l2vpn forwarding bridge-domain bg:bd mac-address location 0/0/CPU0
Fri Nov 29 09:10:07.392 UTC
 To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on LC learned Resync Age/Last Change Mapped
to
-------------- ------- -------                  ---------- -----------     --------------
0010.7777.7777 EVPN    BD id: 0                    N/A        N/A                    N/A

0010.7777.7778 EVPN    BD id: 0                    N/A        N/A                    N/A
```

```
0010.7777.7779 EVPN    BD id: 0                    N/A        N/A                    N/A
```

The show command displays MAC addresses configured through the command-line interface.

```
Router#show l2vpn forwarding bridge-domain bg:bd mac-address location 0/0/CPU0
Fri Nov 29 09:51:19.159 UTC
 To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on LC learned Resync Age/Last Change Mapped
to
-------------- ------- --------                 ----------------------     --------------
0033.0000.0001 static  Te0/0/0/3                   N/A        N/A                    N/A

0033.0000.0002 static  Te0/0/0/3                   N/A        N/A                    N/A

0033.0000.0003 static  Te0/0/0/3                   N/A        N/A                    N/A
```

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information
show l2vpn database, on page 39	Displays L2VPN database
show l2vpn forwarding message counters, on page 47	Displays l2vpn forwarding message counters information.

show l2vpn forwarding message counters

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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:

```
Router# show l2vpn forwarding message counters location 0/RP0/CPU0
Mon Oct 12 14:19:41.768 UTC
Messages exchanged with L2FIB Collaborators:
-------------------------------------------------------------------------------
     Message                                          Count       Info1        Info2
    Time
     =======                                          =====       =====        =====
    ====
     l2vpn provision messages received:                7496       0x800001c    0x0
    Oct 12 13:09:38.477
     l2vpn unprovision messages received:              0          0x0          0x0
    -
     l2vpn bridge provision messages received:         0          0x0          0x0
    -
     l2vpn bridge unprovision messages received:       0          0x0          0x0
    -
     l2vpn bridge main port update messages received:  0          0x0          0x0
    -
     bdxc bridge main port update messages received:   0          0x0          0x0
    -
     l2vpn bridge main port update w/ action=MSTI_DELETE 0        0x0          0x0
    -
     l2vpn bridge main port update ACK sent:           0          0x0          0x0
```

```
-
 bdxc bridge main port update ACK sent:              0          0x0          0x0
-
 l2vpn reception of ACK relay msg received:          0          0x0          0x0
-
 l2vpn bridge port provision messages received:      0          0x0          0x0
-
 l2vpn bridge port unprovision messages received:    0          0x0          0x0
-
 l2vpn shg provision messages received:              0          0x0          0x0
-
 l2vpn shg unprovision messages received:            0          0x0          0x0
-
 l2vpn static mac provision messages received:       0          0x0          0x0
-
 l2vpn static mac unprovision messages received:     0          0x0          0x0
-
 l2vpn static mac flush messages received:           0          0x0          0x0
-
 l2vpn dynamic mac local learning messages received: 0          0x0          0x0
-
 l2vpn dynamic mac local learning dropped queue len: 0          0x0          0x0
-
 l2vpn dynamic mac local learning dropped cache:     0          0x0          0x0
-
 l2vpn dynamic mac local learning dropped multicast: 0          0x0          0x0
-
 l2vpn dynamic mac bcast send failed:                0          0x0          0x0
-
 l2vpn dynamic mac remote learning messages received 0          0x0          0x0
-
 l2vpn dynamic mac refresh messages received:        0          0x0          0x0
-
 l2vpn dynamic mac delete/create messages received:  0          0x0          0x0
-
 l2vpn dynamic mac no-xid dropped:                   0          0x0          0x0
-
 l2vpn dynamic local mac unprovision messages:       0          0x0          0x0
-
 l2vpn dynamic remote mac unprovision messages:      0          0x0          0x0
-
 l2vpn dynamic local mac aged out messages sent:     0          0x0          0x0
-
 l2vpn dynamic mac limit message received:           0          0x0          0x0
-
 l2vpn dynamic mac delete notification:              0          0x0          0x0
-
 l2vpn mac move counter:                             0          0x0          0x0
-
 l2vpn qid mac remote:                               0          0x0          0x0
-
 l2vpn qid mac remote evpn:                          0          0x0          0x0
-
 l2vpn qid mac refresh:                              0          0x0          0x0
-
 l2vpn qid mac learning:                             0          0x0          0x0
-
 AIB update messages received:                       7494       0x8007502    0x8000150
Oct 12 12:49:44.112
 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
-
 l2vpn hw learn MAC update messages received:        0          0x0          0x0
-
 l2vpn hw learn MAC BD limit set messages received:  0          0x0          0x0
-
 l2vpn hw learn MAC BD limit clr messages received:  0          0x0          0x0
-
 l2vpn hw learn MAC BP limit set messages received:  0          0x0          0x0
-
 l2vpn hw learn MAC BP limit clr messages received:  0          0x0          0x0
-
 l2vpn backbone source mac provision msg received:   1          0x0          0x0
Oct 12 12:41:19.807
 l2vpn backbone source mac unprovision msg received: 0          0x0          0x0
-
 l2vpn bridge port MAC flush msg received:           0          0x0          0x0
-
 bdxc ISSU drop msg received:                        0          0x0          0x0
-
 l2vpn ISSU drop msg received:                       0          0x0          0x0
-
 l2vpn BD MAC Flush messages received:               0          0x0          0x0
-
 l2vpn TCN messages received:                        0          0x0          0x0
-
 bdxc G8032 TCN messages transmitted:                0          0x0          0x0
-
 l2fib PD failure count:                             0          0x0          0x0
-
 bdxc DHCP binding provision msg received:           0          0x0          0x0
-
 bdxc DHCP binding unprovision msg received:         0          0x0          0x0
-
 bdxc DHCP configuration msg received:               0          0x0          0x0
-
 platform DAI violation msg received:                0          0x0          0x0
-
 platform IPSG violation msg received:               0          0x0          0x0
-
 platform MAC Secure violation msg received:         0          0x0          0x0
-
 l2vpn g8032 ring provision msg received:            0          0x0          0x0
-
 l2vpn g8032 ring unprovision msg received:          0          0x0          0x0
-
 l2vpn g8032 ring inst provision msg received:       0          0x0          0x0
-
 l2vpn g8032 ring inst unprovision msg received:     0          0x0          0x0
-
 bdxc VPDN L2TPv2 provision msg received:            0          0x0          0x0
-
 bdxc VPDN L2TPv2 unprovision msg received:          0          0x0          0x0
-
 bdxc VPDN L2TPv2 invalid msg received:              0          0x0          0x0
-
 bdxc P2MP PTREE provision msg received:             0          0x0          0x0
-
 bdxc P2MP PTREE unprovision msg received:           0          0x0          0x0
-
 bdxc P2MP PTREE provision msg dropped:              0          0x0          0x0
```

```
-
 bdxc P2MP PTREE unprovision msg dropped:            0          0x0          0x0
-
 l2vpn reception of protection ack msg received:     0          0x0          0x0
-
 l2vpn GLOBAL messages received:                     1          0x0          0x0
Oct 12 12:41:19.807
 l2vpn BD Flush request messages to l2vpn:           0          0x0          0x0
-
 l2vpn evpn mcast provision msg received:            0          0x0          0x0
-
 l2vpn evpn mcast unprovision msg received:          0          0x0          0x0
-
 l2vpn evpn mcast invalid msg received:              0          0x0          0x0
-
 l2vpn evpn mcast unprovision all msg received:      0          0x0          0x0
-
 l2vpn evpn main port provision msg received:        0          0x0          0x0
-
 l2vpn evpn main port unprovision msg received:      0          0x0          0x0
-
 l2vpn evpn main port invalid msg received:          0          0x0          0x0
-
 l2vpn MVRP request:                                 0          0x0          0x0
-
 l2vpn pwgroup status update msg received:           0          0x0          0x0
-
```

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

```
Router# show l2vpn forwarding message counters hardware location 0/$
Mon Oct 12 14:19:59.017 UTC

                        Event Statistics Summary
-----------------------------------------------------------------------
             Create      Modify        Bind       Unbind      Delete
 LOCXC AC      7492        3748        7496            4           0
 VPWS  AC         0           0           0            0           0
 VPLS  AC         0           0           0            0           0
 L2TP  AC         0           0           0            0           0
 VPWS  PW         0           0           0            0           0
 VPLS  PW         0           0           0            0           0
 BRIDGE           0           0           0            0           0
 BRIDGEPORT       0           0           0            0           0
 MAC              0           0           0            0           0
 PBB              0           0           0            0           0
 DHCP             0           0           0            0           0
 L2TP             0           0           0            0           0
 L2TP SESSION     0           0           0            0           0


                     Performance Statistics Summary
-----------------------------------------------------------------------
                  Create     Modify     Delete       Bind     Unbind
 LOCXC AC      000.032 s  000.790 s     < 1 ms  000.810 s  000.003 s
 VPWS  AC         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 VPLS  AC         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 L2TP  AC         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 VPWS  PW         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 VPLS  PW         < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 BRIDGE           < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 BRIDGEPORT       < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
 MAC              < 1 ms     < 1 ms     < 1 ms     < 1 ms     < 1 ms
```

```
PBB              < 1 ms      < 1 ms      < 1 ms      < 1 ms      < 1 ms
DHCP             < 1 ms      < 1 ms      < 1 ms      < 1 ms      < 1 ms
L2TP             < 1 ms      < 1 ms      < 1 ms      < 1 ms      < 1 ms
L2TP SESSION     < 1 ms      < 1 ms      < 1 ms      < 1 ms      < 1 ms
```

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information
show l2vpn database, on page 39	Displays L2VPN database
show l2vpn forwarding, on page 42	Displays forwarding information from the layer2_fib manager on the line card.

show l2vpn index

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

show l2vpn index [**location** | **private**]**private**

Syntax Description

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

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
Router# show l2vpn index
 Mon Oct 12 14:20:20.218 UTC
 Pool id: 0x0, App: AC
   Max number of ID mgr instances: 1
   ID mgr instances in use: 1
   Pool size: 32513
   zombied IDs: 0
   allocated IDs: 3745

 Pool id: 0xfff80002, 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: 0xfff80003, App: MP2MP
   Max number of ID mgr instances: 1
   ID mgr instances in use: 1
   Pool size: 65535
   zombied IDs: 0
```

```
  allocated IDs: 0

Pool id: 0xfff80004, App: RD
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 65536
  zombied IDs: 0
  allocated IDs: 0

Pool id: 0xfff80005, App: IFLIST
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 65535
  zombied IDs: 0
  allocated IDs: 1

Pool id: 0xfff80006, App: ATOM
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 131071
  zombied IDs: 0
  allocated IDs: 0

Pool id: 0xfff80007, App: PWGroup
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 65535
  zombied IDs: 0
  allocated IDs: 1

Pool id: 0xfffd0000, App: Global
  Max number of ID mgr instances: 1
  ID mgr instances in use: 1
  Pool size: 16383
  zombied IDs: 0
  allocated IDs: 2
```

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information
show l2vpn database, on page 39	Displays L2VPN database
show l2vpn forwarding, on page 42	Displays forwarding information from the layer2_fib manager on the line card.

show l2vpn protection main-interface

To display an overview of the main interface or instance operational information, use the **show l2vpn protection main-interface** command in EXEC mode.

show l2vpn protection main-interface [*interface name* {*Interface*}] [**brief** | **detail** | **private**]

Syntax Description

interface name	Interface name of the Ethernet ring G.8032 name.
interface	The forwarding interface ID in number or in Rack/Slot/Instance/Port format as required.
brief	Brief information about the G.8032 ethernet ring configuration.
detail	Information in detail about the G.8032 ethernet ring configuration.
private	Private information about the G.8032 ethernet ring configuration.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.0.1	This command was introduced.
Release 7.7.1	The command output was enhanced to include protection access gateway subtype indication `MST-AG`.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

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

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

Main Interface ID              Subintf Count Protected  Blocked
------------------------------ ------------- ---------- ----------
GigabitEthernet0/0/0/0         1             None       No
   Instance : 0
```

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


Main Interface ID              Subintf Count Protected  Blocked
------------------------------ ------------- ---------- ----------
GigabitEthernet0/0/0/1         1             None       No
   Instance : 0
      State         : FORWARDING
      Sub-Intf #    : 1
      Flush    #    : 0
       Sub-interfaces : GigabitEthernet0/0/0/0.4

RP/0/0/CPU0:ios#show l2vpn protection main-interface gigabitEthernet 0/0/0/1
Tue Mar 15 10:54:13.366 EDT
Main Interface ID              # of subIntf Protected  Protect Type
------------------------------ ------------ ---------- ------------
GigabitEthernet0/0/0/1         2            Yes        MST-AG

   Instance : 0
      State          : FORWARDING
      Sub-Intf #     : 1
      Flush    #     : 1

   Instance : 1
      State          : BLOCKED
      Sub-Intf #     : 1
      Flush    #     : 0

RP/0/0/CPU0:ios#show l2vpn protection main-interface gigabitEthernet 0/0/0/2
Tue Mar 15 10:54:15.044 EDT
Main Interface ID              # of subIntf Protected  Protect Type
------------------------------ ------------ ---------- ------------
GigabitEthernet0/0/0/2         2            Yes        STP

   Instance : 0
      State          : FORWARDING
      Sub-Intf #     : 1
      Flush    #     : 0

   Instance : 1
      State          : FORWARDING
      Sub-Intf #     : 1
      Flush    #     : 0

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

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


RP/0/RSP0/CPU0:router# show l2vpn protection main-interface detail

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/19        4            No

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/20        3            No
```

```
Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/3         2            No

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/30        1            No

Main Interface ID              # of subIntf Protected
------------------------------ ------------ ----------
GigabitEthernet0/1/0/7         4            No


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

Main Interface ID              Ref Count  Protected  Blocked    If Handle  Registered
------------------------------ ---------- ---------- ---------- ---------- ----------
GigabitEthernet0/0/0/0         3          None       No         0x20000020 No

   Instance : 0
      State          : FORWARDING        Config ID  : 0
      Sub-Intf #     : 0                 Ack      # : 0
      Bridge D #     : 0                 N-Ack    # : 0
      Flush    #     : 0                 Rcv      # : 0
      Sub-interfaces : GigabitEthernet0/0/0/0.4

     Instance event trace history [Total events: 1, Max listed: 8]
     ------------------------------------------------------
     Time                Event                          State           Action
     ====                =====                          ========        ========
     01/01/1970 01:00:01 Rcv state IF known             Invalid         134833160
     07/02/2010 10:13:03 Update L2FIB                   FORWARDING      0
     01/01/1970 01:00:25 Rcvd AC MA create + UP I/F ST  FORWARDING      0
```

Related Commands

Command	Description
l2vpn	

show l2vpn resource

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

show l2vpn resource

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
Router# show l2vpn resource
Mon Oct 12 14:21:54.670 UTC
Memory: Normal
```

This table describes the significant fields shown in the display.

Table 2: show l2vpn resource Command Field Descriptions

Field	Description
Memory	Displays memory status.

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information
show l2vpn index, on page 52	Displays statistics about the index manager.

show l2vpn trace

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

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

```
Router# show l2vpn trace
Mon Oct 12 14:22:09.082 UTC
188 unique entries (2596 possible, 0 filtered)
Oct 12 12:37:44.197 l2vpn/policy 0/RP0/CPU0 1# t4349 POLICY:320: l2vpn_policy_reg_agent
started - route_policy_supported=False, forward_class_supported=False
Oct 12 12:39:21.870 l2vpn/fwd-pd 0/RP0/CPU0 1# t5664 FWD_PD:731:
Oct 12 12:39:21.883 l2vpn/fwd-err 0/RP0/CPU0 1# t5664 FWD_ERR|ERR:76: Major version mis-match,
 SHM: 0x0 Expected: 0x1
Oct 12 12:39:21.883 l2vpn/fwd-err 0/RP0/CPU0 1# t5664 FWD_ERR|ERR:87: Magic number mis-match,
 SHM: 0x0 Expected: 0xa7b6c3d8
Oct 12 12:39:21.884 l2vpn/err 0/RP0/CPU0 1# t5664 FWD_ERR|ERR:76: Major version mis-match,
 SHM: 0x0 Expected: 0x1
Oct 12 12:39:21.884 l2vpn/err 0/RP0/CPU0 1# t5664 FWD_ERR|ERR:87: Magic number mis-match,
SHM: 0x0 Expected: 0xa7b6c3d8
Oct 12 12:39:21.890 l2vpn/fwd-detail 0/RP0/CPU0 1# t5664 FWD_DETAIL:263: PWGROUP Table init
 succeeded
Oct 12 12:39:21.890 l2vpn/fwd-detail 0/RP0/CPU0 2# t5664 FWD_DETAIL:416: l2tp session table
 rebuilt
Oct 12 12:39:21.903 l2vpn/fwd-common 0/RP0/CPU0 1# t5664 FWD_COMMON:39: L2FIB_OBJ_TRACE:
trace_buf=0x7d48e0
Oct 12 12:39:25.613 l2vpn/issu 0/RP0/CPU0 1# t5664 ISSU:790: ISSU - iMDR init called;
'infra/imdr' detected the 'informational' condition 'the service is not supported in the
node'
Oct 12 12:39:25.613 l2vpn/issu 0/RP0/CPU0 1# t5664 ISSU:430: ISSU - attempt to start
COLLABORATOR wait timer while not in ISSU mode
Oct 12 12:39:25.638 l2vpn/fwd-common 0/RP0/CPU0 1# t5664 FWD_COMMON:4241: show edm thread
initialized
Oct 12 12:39:25.781 l2vpn/fwd-mac 0/RP0/CPU0 1# t5664 FWD_MAC|ERR:783: Mac aging init
Oct 12 12:39:25.781 l2vpn/fwd-mac 0/RP0/CPU0 2# t5664 FWD_MAC:1954: l2vpn_gsp_cons_init
returned Success
Oct 12 12:39:25.781 l2vpn/err 0/RP0/CPU0 1# t5664 FWD_MAC|ERR:783: Mac aging init
Oct 12 12:39:25.782 l2vpn/fwd-aib 0/RP0/CPU0 4# t5664 FWD_AIB:446: aib connection opened
successfully
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 2# t5664 FWD_MAC:2004: Client successfully
joined gsp group
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 1# t5664 FWD_MAC:781: Initializing the txlist
 IPC thread
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 1# t5664 FWD_MAC:3195: gsp_optimal_msg_size =
 31264 (real: True)
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 1# t5664 FWD_MAC:626: Entering mac aging timer
 init
Oct 12 12:39:25.783 l2vpn/fwd-mac 0/RP0/CPU0 1# t7519 FWD_MAC:725: Entering event loop for
 mac txlist thread
Oct 12 12:39:25.797 l2vpn/fwd-mac 0/RP0/CPU0 1# t4222 FWD_MAC:2221: learning_client_colocated
 0, is_client_netio 1
```

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information
show l2vpn index, on page 52	Displays statistics about the index manager.

Command	Description
show l2vpn resource, on page 57	Displays the memory state in the L2VPN process.

show l2vpn xconnect

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

show l2vpn xconnect [**brief** | **detail***encapsulation* | **group** | **groups** | **interface** | **location** | **neighbor** | **standby** | **state** | **summary** | **type locally-switched**]

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.
neighbor	(Optional) Filters on neighbor.
private	(Optional) Displays private information.
standby	(Optional) Displays standby node specific information.
state	(Optional) Filters the following xconnect state types: • up • down
summary	(Optional) Displays AC information from the AC Manager database.
type	(Optional) Filters the locally switched xconnect type.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.
Release 7.4.1	This command was modified to include `(SI) Seamless Inactive` status in the show output.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
Router# show l2vpn xconnect
Mon Oct 12 14:22:20.566 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
XConnect                   Segment 1                       Segment 2
Group      Name       ST   Description            ST       Description            ST
------------------------   ------------------------------   ------------------------------
XC         XC         UP   BE1                    UP       BE2                    UP
-------------------------------------------------------------------------------------------
XCON31     XCON1_P2P1 UP   Te0/0/0/0.1            UP       Te0/0/0/26.1           UP
-------------------------------------------------------------------------------------------
XCON32     XCON1_P2P2 UP   Te0/0/0/0.2            UP       Te0/0/0/26.2           UP
-------------------------------------------------------------------------------------------
XCON33     XCON1_P2P3 UP   Te0/0/0/0.3            UP       Te0/0/0/26.3           UP
-------------------------------------------------------------------------------------------
XCON34     XCON1_P2P4 UP   Te0/0/0/0.4            UP       Te0/0/0/26.4           UP
-------------------------------------------------------------------------------------------
XCON35     XCON1_P2P5 UP   Te0/0/0/0.5            UP       Te0/0/0/26.5           UP
-------------------------------------------------------------------------------------------
XCON36     XCON1_P2P6 UP   Te0/0/0/0.6            UP       Te0/0/0/26.6           UP
-------------------------------------------------------------------------------------------
XCON37     XCON1_P2P7 UP   Te0/0/0/0.7            UP       Te0/0/0/26.7           UP
-------------------------------------------------------------------------------------------
XCON38     XCON1_P2P8 UP   Te0/0/0/0.8            UP       Te0/0/0/26.8           UP
-------------------------------------------------------------------------------------------
```

This example shows the output of the **show run l2vpn** command :

```
Router# show run l2vpn

Mon Oct 12 14:23:24.723 UTC
l2vpn
 xconnect group XC
  p2p XC
   interface Bundle-Ether1
   interface Bundle-Ether2
  !
 !
 xconnect group XCON31
  p2p XCON1_P2P1
   interface TenGigE0/0/0/0.1
   interface TenGigE0/0/0/26.1
  !
 !
 xconnect group XCON32
  p2p XCON1_P2P2
   interface TenGigE0/0/0/0.2
   interface TenGigE0/0/0/26.2
  !
 !
 xconnect group XCON33
  p2p XCON1_P2P3
```

```
   interface TenGigE0/0/0/0.3
   interface TenGigE0/0/0/26.3

RP/0/RSP1/CPU0:14A1#show l2vpn xconnect pw-id 11
Thu Feb 25 11:57:27.622 EST
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed,
        LU = Local Up, RU = Remote Up, CO = Connected, (SI) = Seamless Inactive

XConnect                   Segment 1                       Segment 2
Group      Name       ST   Description            ST       Description            ST
------------------------   ----------------------------   ----------------------------
evpn-vpws  test11-1   UP   BE11                   UP       EVPN 11,11,24048       UP
-------------------------------------------------------------------------------------
legacy-tldp
           test11     DN   BE11                   SB(SI)   192.168.12.110  11     UP
-------------------------------------------------------------------------------------
```

This table describes the significant fields shown in the display.

Table 3: show l2vpn xconnect Command Field Descriptions

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

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information
show l2vpn database, on page 39	Displays L2VPN database
show l2vpn pw-class, on page 64	Displays L2VPN pseudowire class information.

show l2vpn pw-class

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

show l2vpn pw-class [**detail** | **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 mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
l2vpn	read

Examples

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

```
Router# show l2vpn pw-class

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

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

```
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 10.0.0.1
```

This table describes the significant fields shown in the display.

Table 4: show l2vpn pw-class Command Field Descriptions

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

Related Commands

Command	Description
l2vpn, on page 17	Enters L2VPN configuration mode.
p2p, on page 24	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 25	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 31	Displays L2VPN information
show l2vpn database, on page 39	Displays L2VPN database

storm-control

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.

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

Syntax Description

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

Command Default

Storm control is disabled by default.

Command Modes

l2vpn bridge group bridge-domain access circuit configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

- The storm control configuration is supported only on one sub-interface under a main interface, though the system allows you to configure storm control on more than one sub-interface. However, only the first storm control configuration under a main interface takes effect, though the running configuration shows all the storm control configurations that are committed. After reload, any of the storm control configurations may take effect irrespective of the order of configuration.
- Starting from 7.8.1, you can enable per subinterface configuration support for storm control by using the **hw-module storm-control-combine-policer-bw enable** command.
- System supports storm control per-EFP.
- If storm control is applied on one bridge port, you cannot apply storm control on another bridge port or sub-interface under the same main-port. On configuring, system pop-ups an error, but needs to be manually unconfigured.

- System does not support storm control on pseudowire bridge-ports.
- Storm control counters are not supported
- Only kbps rate is supported by hardware. Though the pps configuration is allowed, it is converted to kbps. The pps rate is calculated as 1 pps = 8 kbps.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group csco
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet0/1/0/0.100
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# storm-control broadcast kbps 4500
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# commit
```

vlan-switch vsp

To configure a VLAN switch profile and assign VLAN IDs to the profile, use the **vlan-switch vsp** command in L2VPN configuration mode.

vlan-switch vsp

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 26.2.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to create a VLAN switch profile :

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# vlan-switch vsp
Router(config-l2vpn-vs)# vlan 2001-2010
Router(config-l2vpn-vs)# commit
```

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 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to group all cross-connects for XCON1:

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface gigabitethernet0/1/0/0.1
Router(config-l2vpn-xc-p2p)# neighbor 10.165.100.151 pw-id 100
Router(config-l2vpn-xc-p2p-pw)# mpls static label local 50 remote 40
Router(config-l2vpn-xc-p2p-pw)# commit
```

Related Commands

Command	Description
interface (p2p), on page 3	Configures an attachment circuit.
l2vpn, on page 17	Enters L2VPN configuration mode.

Command	Description
show l2vpn, on page 31	Displays L2VPN information
show l2vpn xconnect, on page 61	Displays brief information on configured cross-connects.