VPN and Ethernet Services Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers

First Published: 2016-04-27

Last Modified: 2023-12-01

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

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

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

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

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

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

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

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

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

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

© 2016–2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

This preface contains these sections:

Changes to This Document

This table lists the technical changes made to this document since it was first released.

Table 1: Changes to This Document

Date	Summary
April 2016	Initial release of this document.
November 2016	Republished with documentation updates for Release 6.1.2 features.
July 2017	Republished with documentation updates for Release 6.2.2 features.
September 2017	Republished with documentation updates for Release 6.3.1 features.
March 2019	Republished with documentation updates for Release 6.5.3 features.
May 2019	Republished with documentation updates for Release 6.6.25 features.
January 2020	Republished with documentation updates for Release 7.1.1 features.
August 2020	Republished with documentation updates for Release 7.2.1 features.
February 2021	Republished with documentation updates for Release 7.3.1 features.

Date	Summary
July 2021	Republished with documentation updates for Release 7.4.1 features.
April 2022	Republished with documentation updates for Release 7.5.2 features.
July 2022	Republished with documentation updates for Release 7.7.1 features.
November 2022	Republished with documentation updates for Release 7.8.1 features.
April 2023	Republished with documentation updates for Release 7.9.1 features.
August 2023	Republished with documentation updates for Release 7.10.1 features.
December 2023	Republished with documentation updates for Release 7.11.1 features.

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Gigabit Ethernet Interfaces Commands

This section describes the commands used to configure Gigabit Ethernet 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 Gigabit Ethernet for Layer 2 VPNs 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*.

dot1q tunneling ethertype

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
vlan	read, write

Examples

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

```
Router# configure
Router(config)# interface GigabitEthernet 0/1/5/0
Router(config-if)# dot1q tunneling ethertype 0x9100
```

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

```
Router# configure
```

```
Router(config)# interface GigabitEthernet 0/1/5/1
Router(config-if)# dot1q tunneling ethertype 0x9200
```

Related Commands

Command	Description
encapsulation dot1q, on page 32	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 36	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1ad, on page 34	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1ad dot1q, on page 38	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.

l2transport (Ethernet)

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

l2transport
no l2transport

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Sub-interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The l2transport command and these configuration items are mutually exclusive:

- IPv4 address and L3 feature configuration
- IPv4 enable and L3 feature configuration
- Bundle-enabling configuration
- L3 sub-interfaces
- Layer 3 QoS Policy

Note

- After an interface or connection is set to Layer 2 switched, commands such as **ipv4 address** are not usable. If you configure routing commands on the interface, **l2transport** is rejected.
- The **l2transport** command is mutually exclusive with any Layer 3 interface configuration.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
Router# configure
Router(config)# interface TenGigE 0/2/0/0
```

```
Router(config-if)# l2transport
Router(config-if-l2)#
```

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

The following example shows how to use the l2transport command on an Ethernet sub-interface:

```
Router# configure
Router(config)# interface TenGigE 0/1/0/3.10 l2transport
Router(config-subif)# encapsulation dot1q 10
```

Examples

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

Ethernet Port Mode:

```
Router# configure
Router(config)# interface TenGigE 0/0/0/10
Router(config-if)# l2transport
```

Ethernet VLAN Mode:

```
Router# configure
Router(config)# interface TenGigE 0/0/0/0.1 l2transport
Router(config-if)# encapsulation dot1q 10
```

Ethernet VLAN Mode (QinQ):

```
Router# configure
Router(config)# interface TenGigE 0/0/0/0.1 l2transport
Router(config-if)# encapsulation dot1q 10 second-dot1q 11
```

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

Related Commands

Command	Description
encapsulation dot1q, on page 32	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 36	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.

l2transport propagate

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

l2transportpropagateremote-status
no l2transportpropagatepropagateremote-status

Syntax Description

remote-status	Propagates remote link status changes.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

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

To display the state of l2transport events, use the **show controller internal** command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/RP0/CPU0:router(config-if)# l2transport propagate remote remote-status
```

Related Commands

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

l2protocol (l2pt)

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

l2protocol cpsv tunnel
no l2protocol

Syntax Description

cpsv Enables L2PT for the interface. L2PT is enabled for the following protocols only:

- CDP
- STP
- VTP

Note STP includes all Spanning Tree protocol derivatives (RSTP, MSTP, etc.)

tunnel Performs L2PT encapsulation on frames as they enter the interface. Also, performs L2PT de-encapsulation on frames as they exit they interface.

L2PT encapsulation rewrites the destination MAC address with the L2PT destination MAC address. L2PT deencapsulation replaces the L2PT destination MAC address with the original destination MAC address.

Command Default

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

Command Modes

Layer 2 transport configuration

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
l2vpn	read, write

Examples

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

```
Router# configure
Router(config)# interface TenGigE 0/0/0/1
```

```
Router(config-if)# l2transport
Router(config-if-l2)# l2protocol cpsv tunnel
```

ethernet lmi

To enable Ethernet Local Management Interface (E-LMI) operation on an interface and enter interface Ethernet LMI configuration mode, use the **ethernet lmi** command in interface configuration mode. To disable Ethernet LMI and return to the default, use the **no** form of the command.

ethernet lmi
no ethernet lmi

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet LMI is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

Ethernet LMI is supported only on physical Ethernet interfaces.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to enable Ethernet LMI on a Gigabit Ethernet interface and enter Ethernet LMI configuration mode:

```
Router# interface gigabitethernet 0/1/0/0
Router(config-if)# ethernet lmi
Router config-if-elmi)# commit
```

ethernet loopback

To enable Ethernet data plane loopback on an interface, use the **ethernet loopback** command in interface or sub-interface configuration mode. To disable Ethernet data plane loopback on an interface, use the **no** form of this command.

ethernet loopback permit [**internal** | **external**]
no ethernet loopback permit [**internal** | **external**]

Command Default

None

Command Modes

Interface configuration

Sub-interface configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows how you can configure Ethernet Data Plane Loopback:

```
/* Configuring External Loopback */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tenGigE 0/0/0/0 l2transport
RP/0/RSP0/CPU0:router(config-subif)#  ethernet loopback permit external

/* Configuring Internal Loopback */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tenGigE 0/0/0/1 l2tansport
RP/0/RSP0/CPU0:router(config-subif)# ethernet loopback permit internal
```

flood mode ac-ingress-replication

To add BUM traffic queueing support for attachment circuits in a bridge domain, use the **flood mode ac-ingress-replication** command in the L2VPN bridge group bridge domain configuration mode. To return to the default behavior, use the **no** form of this command.

flood mode ac-ingress-replication

This command has no keywords or arguments.

Command Default

BUM traffic queueing support is not supported for attachment circuits in a bridge domain.

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 7.2.1	This command was introduced.
Release 7.2.2	This command was deprecated.

Usage Guidelines

BUM traffic queueing support for attachment circuits in a bridge domain is not supported on devices that have multiple NPUs or line cards. It is only supported on single NPU devices.

Perform this task to add BUM traffic queueing support for attachment circuits in a bridge domain

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 10
Router(config-l2vpn-bg)# bridge-domain 1
Router(config-l2vpn-bg-bd)# flood mode ac-ingress-replication
Router(config-l2vpn-bg-bd)# commit
```

show ethernet cfm peer meps

To display information about maintenance end points (MEPs) for peer MEPs, use the **show ethernet cfm peer meps** command in EXEC mode.

show ethernet cfm peer meps [{**domain** *domain-name* [**service** *service-name* [**local mep-id** *id* [**peer** {**mep-id** *id* | **mac-address** *H . H . H*}]]] | **interface** *type interface-path-id* [**domain** *domain-name* [**peer** {**mep-id** *id* | **mac-address** *H . H . H*}]]}] [{**cross-check** [{**missing** | **unexpected**}] | **errors**}] [**detail**]

Syntax Description

cross-check	(Optional) Displays information about peer MEPs with cross-check errors.
detail	(Optional) Displays detailed information.
domain *domain-name*	(Optional) Displays information about a CFM domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
errors	(Optional) Displays information about peer MEPs with errors.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
local mep-id *id*	(Optional) Displays information about a local MEP, where *id* is the number of the MEP.
missing	(Optional) Displays information about peer MEPs that are missing.
peer mep-id *id*	(Optional) Displays information about a peer MEP, where *id* is the number of the MEP.
peer mac-address *H.H.H*	(Optional) Displays information about a peer MEP, where *H.H.H* is the hexadecimal address of the MEP.
service *service-name*	(Optional) Displays information about a CFM service, where *service-name* is a string of a maximum of 154 characters that identifies the maintenance association to which the maintenance points belong.
unexpected	(Optional) Displays information about unexpected peer MEPs.

Command Default

Peer MEPs for all domains are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

Note If a Local MEP is receiving Wrong Level CCMs, and if the Remote MEP has its CCM processing offloaded, then the last CCM cannot be displayed.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows sample output of MEPs detected by a local MEP:

```
Router# show ethernet cfm peer meps

Flags:
> - Ok                          I - Wrong interval
R - Remote Defect received      V - Wrong level
L - Loop (our MAC received)     T - Timed out
C - Config (our ID received)    M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
* - Multiple errors received

Domain dom3 (level 5), Service ser3
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
St     ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ------------ --------- ------ ----- -----
V      10 0001.0203.0403 Up      00:01:35            2      0     0     2

Domain dom4 (level 2), Service ser4
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
St     ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ------------ --------- ------ ----- -----
 >     20 0001.0203.0402 Up      00:00:03            4      1     0     0
 >     21 0001.0203.0403 Up      00:00:04            3      0     0     0

Domain dom5 (level 2), Service dom5
```

Table 2: show ethernet cfm peer meps Field Descriptions

St	Status: one or two characters, representing the states listed at the top of the output.
ID	Peer MEP ID
MAC address	Peer MAC Address. If this entry is a configured cross-check MEP, with no MAC address specified, and no CCMs are currently being received from a peer MEP with a matching MEP ID, then this field is blank.

Port	Port state of the peer, based on the Port Status and Interface Status TLVs. If no TLVs or CCMs have been received, this field is blank. Otherwise, the port status is displayed—unless it is Up. If the port status is Up, then the interface status is displayed.
Up/Downtime	Time since the peer MEP last came up or went down. If CCMs are currently being received, it is the time since the peer MEP last came up, which is the time since the first CCM was received. If CCMs are not currently being received, it is the time since the peer MEP last went down, which is the time since the loss threshold was exceeded and a loss of continuity was detected.
CcmRcvd	Total number of CCMs received from this peer MEP.
SeqErr	Number of CCMs received out-of-sequence.
RDI	Number of CCMs received with the RDI bit set.
Error	Number of CCMs received with CCM defects, such as: • Invalid level error • Maintenance Association Identifier (MAID) error • Interval error • Received with out MEP ID error • Invalid source MAC error

This example shows sample detailed output of MEPs detected by a local MEP:

```
Router# show ethernet cfm peer meps detail

Domain dom3 (level 5), Service ser3
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
Peer MEP-ID 10, MAC 0001.0203.0403
   CFM state: Wrong level, for 00:01:34
   Port state: Up
   CCM defects detected:    V - Wrong Level
   CCMs received: 5
     Out-of-sequence:             0
     Remote Defect received:      5
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              5
     Loop (our MAC received):     0
     Config (our ID received):    0
Last CCM received
     Level: 4, Version: 0, Interval: 1min
     Sequence number: 5, MEP-ID: 10
     MAID: String: dom3, String: ser3
     Port status: Up, Interface status: Up


Domain dom4 (level 2), Service ser4
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
Peer MEP-ID 20, MAC 0001.0203.0402
```

```
   CFM state: Ok, for 00:00:04
   Received CCM handling offloaded to software
   Port state: Up
   CCMs received: 7
     Out-of-sequence:             1
     Remote Defect received:      0
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              0
     Loop (our MAC received):     0
 Config (our ID received):    0
Last CCM received
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 20
     MAID: String: dom4, String: ser4
     Chassis ID: Local: ios; Management address: 'Not specified'
     Port status: Up, Interface status: Up

Peer MEP-ID 21, MAC 0001.0203.0403
   CFM state: Ok, for 00:00:05
   Port state: Up
   CCMs received: 6
     Out-of-sequence:             0
     Remote Defect received:      0
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              0
     Loop (our MAC received):     0
     Config (our ID received):    0
Last CCM received 00:00:05 ago:
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 21
     MAID: String: dom4, String: ser4
     Port status: Up, Interface status: Up


Domain dom5 (level 2), Service ser5
Up MEP on Standby Bundle-Ether 1 MEP-ID 1
================================================================================
Peer MEP-ID 600, MAC 0001.0203.0401
   CFM state: Ok (Standby), for 00:00:08, RDI received
   Port state: Down
   CCM defects detected:    Defects below ignored on local standby MEP
                            I - Wrong Interval
                            R - Remote Defect received
   CCMs received: 5
     Out-of-sequence:             0
     Remote Defect received:   5
 Wrong Level:                 0
     Cross-connect W(wrong MAID): 0
     Wrong Interval:              5
     Loop (our MAC received):     0
     Config (our ID received):    0
   Last CCM received 00:00:08 ago:
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 600
     MAID: DNS-like: dom5, String: ser5
     Chassis ID: Local: ios; Management address: 'Not specified'
     Port status: Up, Interface status: Down

Peer MEP-ID 601, MAC 0001.0203.0402
   CFM state: Timed Out (Standby), for 00:15:14, RDI received
   Port state: Down
   CCM defects detected:    Defects below ignored on local standby MEP
```

```
                        I - Wrong Interval
                        R - Remote Defect received
                        T - Timed Out
                        P - Peer port down
CCMs received: 2
  Out-of-sequence:             0
  Remote Defect received:      2
  Wrong Level:                 0
  Cross-connect (wrong MAID):  0
  Wrong Interval:              2
  Loop (our MAC received):     0
  Config (our ID received):    0
Last CCM received 00:15:49 ago:
  Level: 2, Version: 0, Interval: 10s
  Sequence number: 1, MEP-ID: 600
  MAID: DNS-like: dom5, String: ser5
  Chassis ID: Local: ios; Management address: 'Not specified'
  Port status: Up, Interface status: Down
```

Table 3: show ethernet cfm peer meps detail Field Descriptions

CFM state	State of the peer MEP, how long it has been up or down, and whether the RDI bit was set in the last received CCM. The following possible states are shown if CCMs are currently being received: • Missing • Timed out—No CCMs have been received for the loss time • Ok • Indication of a defect
Port state	Port state of the peer, based on the Port Status and Interface Status TLVs. If no TLVs or CCMs have been received, this field is blank. Otherwise, the port status is displayed—unless it is Up. If the port status is Up, then the interface status is displayed.

CCM defects detected	Types of CCM defects that have been detected. The possible defects are: • Remote Defect re ceived—The last CCM received from the peer had the RDI bit set. • Loop (our MAC received)—CCMs were received from a peer with the same MAC address as the local MEP. • Config (our ID received)—CCMs were received from a peer with the same MEP ID as the local MEP. • Cross-connect (wrong MAID)—The last CCM received from the peer contained a domain/service identified that did not match the locally configured domain/service identifier. • Peer port down—The last CCM received from the peer contained an Interface Status indicating that the interface on the peer was not up. • Wrong interval—The last CCM received contained a CCM interval that did not match the locally configured CCM interval. • Wrong level—The last CCM received was for a lower level than the level of the local MEP. • Timed out—No CCMs have been received within the loss time. • Missing (cross-check)—Cross-check is configured and lists this peer MEP, but no CCMs have been received within the loss time. • Unexpected (cross-check)—Cross check is configured for this service and does not list this peer MEP, but CCMs have been received from it within the loss time.
CCMs received	Number of CCMs received in total, by defect type.
Last CCM received	How long ago the last CCM was received, and a full decode of its contents. Any unknown TLVs are displayed in hexadecimal.
Offload status	Offload status of received CCM handling.

show ethernet lmi interfaces

To display Ethernet Local Management Interface (E-LMI) information for an interface, including protocol status and error and event statistics, use the **show ethernet lmi interfaces** command in EXEC configuration mode.

show ethernet lmi interfaces [*type interface-path-id*][**brief** | **detail**]
show ethernet lmi interfaces [**brief** | **detail**][**location** *location*]

Syntax Description

brief	(Optional) Displays summary information about the E-LMI protocol status, number of EVCs and errors, and CE-VLAN/EVC map type.
detail	(Optional) Displays the configured and operational state of E-LMI on the interface, with counts for reliability and protocol errors and elapsed time since various events have occurred, including details about subinterfaces and EVC status.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *location*	(Optional) Displays E-LMI information for the designated node. The *location* argument is entered in the *rack*/*slot*/*module* notation. **Note** The location cannot be specified when you specify an interface type.

Command Default

The output displays the configured and operational state of E-LMI on the interface, with counts for reliability and protocol errors and elapsed time since various events have occurred since the protocol was enabled on the interface or counters were cleared.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

If Protocol Errors are seen in the output, then the CE device is sending packets to the PE device, but the PE does not understand those packets. This suggests an incorrect implementation of the E-LMI protocol on the

CE side, or corruption of the packets on the path between the CE and PE. E-LMI packets have a strictly defined structure in the MEF 16 standard, and any deviation from that results in a protocol error. The PE will not respond to any packets that are malformed and result in a protocol error.

The Reliability Error counters can indicate that messages are being lost between the PE and CE devices. The timers in the last block of the output should indicate that messages are being sent and received by the PE device. Consider the following actions when these Reliability Errors occur:

- Status Enquiry Timeouts—If this counter is continuously incrementing, it indicates that the Polling Timer on the CE is configured to a greater value than the Polling Verification Timer (PVT) configuration on the PE. Status Enquiry messages will be sent less frequently than the PVT expects them and PVT timeouts occur. Be sure that the value of the PVT (specified by the **polling-verification-timer** command on the PE) is greater than the Polling Timer value on the CE device.
- Invalid Sequence Number—Indicates that messages from the PE are not being received by the CE. Be sure that the correct interface on the CE device is connected to the corresponding E-LMI interface on the PE device, so that communication can take place. Verify that both interfaces are Up.
- Invalid Report Type—This error can occur under the following conditions:
  - If the protocol is in the process of a status update and an "E-LMI Check" type of STATUS ENQUIRY is received by the PE, then the PE ignores the ENQUIRY and records an error.
  - If the protocol is not in the process of a status update and a "Full Status Continued" type of STATUS ENQUIRY is received by the PE, then the PE ignores the ENQUIRY and records an error.

Note If the protocol is in the process of a status update and a "Full Status" type of STATUS ENQUIRY is received by the PE, then the PE restarts the status update but does not record any error.

Task ID

Task ID	Operation
ethernet-services	read

The following example shows sample output for the default form of the command:

```
Router# show ethernet lmi interfaces
Interface: GigabitEthernet0/0/0/0
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-Slot1-Port0
  Line Protocol State: Up
  MTU: 1500 (2 PDUs reqd. for full report)
  CE-VLAN/EVC Map Type: Bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 1732
  Last Sequence Numbers: Sent 128, Received 128

  Reliability Errors:
    Status Enq Timeouts                19 Invalid Sequence Number            0
    Invalid Report Type                 0

  Protocol Errors:
    Malformed PDUs                      0 Invalid Protocol Version           0
    Invalid Message Type                0 Out of Sequence IE                 0
    Duplicated IE                       0 Mandatory IE Missing               0
```

```
  Invalid Mandatory IE                0 Invalid non-Mandatory IE           0
  Unrecognized IE                     0 Unexpected IE                      0

Full Status Enq Rcvd     00:00:10 ago   Full Status Sent      00:00:10 ago
PDU Rcvd                 00:00:00 ago   PDU Sent              00:00:00 ago
LMI Link Status Changed  10:00:00 ago   Last Protocol Error      never
Counters cleared            never
```

Table 4: show ethernet lmi interfaces Field Descriptions

Field	Description
Interface:	Name of the interface running the E-LMI protocol.
Ether LMI Link Status:	Status of the E-LMI protocol on the interface. Possible values are Up, Down, or Unknown (PVT disabled).
UNI Id:	Name of the UNI as configured by the **ethernet uni id** command. This output field does not appear if the UNI ID is not configured.
Line Protocol State:	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
MTU (*x* PDUs reqd for full report)	Maximum Transmission Unit of the interface and the number (*x*) of E-LMI PDUs of that size required to send one full status report.
CE-VLAN/EVC Map Type: *type* (*x* EVCs)	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible values for *type* are Bundling, All to One Bundling, or Service Multiplexing with no bundling. The number *x* of EVCs in the map are displayed in parentheses.
Configuration: Status counter	Value of the MEF N393 Status Counter as configured by the **status-counter** command.
Polling Verification Timer	Value of the MEF T392 Polling Verification Timer (in seconds) as configured by the **polling-verification-timer** command. Displays "disabled" if the PVT is turned off.
Last Data Instance Sent:	Current value of the Data Instance.
Last Sequence Numbers: Sent *x*, Received *y*	Values of the last sent (*x*) and received (*y*) sequence numbers as reported in sent PDUs.

Field	Description
Reliability Errors:	Number of times the specified types of reliability errors have occurred since the protocol was enabled on the interface or counters were cleared: • Status Enq Timeouts—Increments every time the Polling Verification Timer (PVT) expires. • Invalid Report Type—Increments if the Report Type is not appropriate to the protocol's current state. There are four Report Types defined by the E-LMI Standard, and only three of them can appear in Status Enquiry messages that the PE receives. These are: E-LMI Check, Full Status and Full Status Continued. • Invalid Sequence Number—Increments whenever the received sequence number in a Status Enquiry from the CE does not match the last sent sequence number in the PE response. Indicates that messages from the PE are not being received by the CE. The PE continues to respond with the requested Report Type. For more information about possible actions, see the "Usage Guidelines" section.
Protocol Errors: (Malformed PDUs, Invalid Message Type, Duplicated IE, and others)	Number of times the specified types of protocol errors have occurred since the protocol was enabled on the interface or counters were cleared.
Full Status Enq Rcvd, PDU Rcvd, LMI Link Status Changed, Counters cleared, Full Status Sent, PDU Sent, and Last Protocol Error.	Elapsed time (hrs:mins:secs ago) since the specified events last occurred or counters were cleared. Displays "never" if the event has not occurred since the protocol was enabled on the interface or counters were cleared.

The following example shows sample output for the **show ethernet lmi interfaces brief** form of the command:

```
Router# show ethernet lmi interfaces brief
                     ELMI   LineP      #           CE-VLAN/
Interface            State  State      EVCs  Errors EVC Map
------------------------------------------------------------------------------
Gi0/0/0/0            Up     Up            3      19 Multiplexing, no bundling
Gi0/0/0/1            Down   Admin-down    1       0 All to One Bundling
```

Table 5: show ethernet lmi interfaces brief Field Descriptions

Field	Description
Interface	Name of the interface running the E-LMI protocol.

Field	Description
ELMI State	Status of the E-LMI protocol. Possible values are Up, Down, or N/A if the Polling Verification Timer is disabled.
LineP State	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
# EVCs	Total number of EVCs in the CE-VLAN/EVC map.
Errors	Total number of reliability and protocol errors encountered since the protocol was enabled on the interface or counters were cleared.
CE-VLAN/EVC Map	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible values are Bundling, All to One Bundling, or Multiplexing, no bundling.

The following example shows sample output for the **show ethernet lmi interfaces detail** form of the command:

```
Router#show ethernet lmi interfaces detail
Interface: GigabitEthernet0/0/0/0
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-Slot1-Port0
  Line Protocol State: Up
  MTU: 1500 (2 PDUs reqd. for full report)
  CE-VLAN/EVC Map Type: Bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 1732
  Last Sequence Numbers: Sent 128, Received 128

  Reliability Errors:
    Status Enq Timeouts                 19 Invalid Sequence Number             0
    Invalid Report Type                  0

  Protocol Errors:
    Malformed PDUs                       0 Invalid Protocol Version            0
    Invalid Message Type                 0 Out of Sequence IE                  0
    Duplicated IE                        0 Mandatory IE Missing                0
    Invalid Mandatory IE                 0 Invalid non-Mandatory IE            0
    Unrecognized IE                      0 Unexpected IE                       0

  Full Status Enq Rcvd     00:00:10 ago   Full Status Sent      00:00:10 ago
  PDU Rcvd                 00:00:00 ago   PDU Sent              00:00:00 ago
  LMI Link Status Changed  10:00:00 ago   Last Protocol Error      never
  Counters cleared            never

  Sub-interface: GigabitEthernet0/0/0/0.1
    VLANs: 1,10,20-30, default, untagged/priority tagged
    EVC Status: New, Partially Active
    EVC Type: Multipoint-to-Multipoint
    OAM Protocol: CFM
      CFM Domain: Global (level 5)
      CFM Service: CustomerA
    Remote UNI Count: Configured = 2, Active = 1

    Remote UNI Id                                                    Status
```

```
-------------                                                   ------
PE2-CustA-Slot2-Port2                                           Up
PE2-CustA-Slot3-Port3                                           Unreachable
```

Table 6: show ethernet lmi interfaces detail Field Descriptions

Field	Description
Interface:	Name of the interface running the E-LMI protocol.
Ether LMI Link Status:	Status of the E-LMI protocol on the interface. Possible values are Up, Down, or Unknown (PVT disabled).
UNI Id:	Name of the UNI as configured by the **ethernet uni id** command. This output field does not appear if the UNI ID is not configured.
Line Protocol State:	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
MTU (*x* PDUs reqd for full report)	Maximum Transmission Unit of the interface and the number (*x*) of E-LMI PDUs of that size required to send one full status report.
CE-VLAN/EVC Map Type: *type* (*x* EVCs)	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible values for *type* are Bundling, All to One Bundling, or Service Multiplexing with no bundling. The number *x* of EVCs in the map are displayed in parentheses.
Configuration: Status counter	Value of the MEF N393 Status Counter as configured by the **status-counter** command.
Polling Verification Timer	Value of the MEF T392 Polling Verification Timer (in seconds) as configured by the **polling-verification-timer** command. Displays "disabled" if the PVT is turned off.
Last Data Instance Sent:	Current value of the Data Instance.
Last Sequence Numbers: Sent *x*, Received *y*	Values of the last sent (*x*) and received (*y*) sequence numbers as reported in sent PDUs.
Reliability Errors: (Status Enq Timeouts, Invalid Report Type, and Invalid Sequence Number)	Number of times the specified types of reliability errors have occurred since the protocol was enabled on the interface or counters were cleared.
Protocol Errors: (Malformed PDUs, Invalid Message Type, Duplicated IE, and others)	Number of times the specified types of protocol errors have occurred since the protocol was enabled on the interface or counters were cleared.

Field	Description
Full Status Enq Rcvd, PDU Rcvd, LMI Link Status Changed, Counters cleared, Full Status Sent, PDU Sent, and Last Protocol Error.	Elapsed time (hrs:mins:secs ago) since the specified events last occurred or counters were cleared. Displays "never" if the event has not occurred since the protocol was enabled on the interface or counters were cleared.
Subinterface:	Name of the subinterface corresponding to the EVC.
VLANs:	VLAN traffic on the interface that corresponds to the EFPs encapsulation, with the following possible values: • Numbers of the matching VLAN IDs **Note** If Q-in-Q encapsulation is configured, only the outer tag is displayed. • default—Indicates that Default tagging is configured, or the encapsulation specifies to match "any." • none—No matches for the configured encapsulation have occurred on the interface. • untagged/priority—Traffic is either untagged or has priority tagging. **Note** If the message "EVC omitted from Full Status due to encapsulation conflict" is displayed above the VLAN output, a misconfiguration has occurred with two or more EFPs having a conflicting encapsulation.
EVC Status:	State of the EVC, with the following possible values: • Active—E-LMI is operational for this EVC. • Inactive—All of the remote UNIs are unreachable or down. • New—The EVC has not yet been reported to the CE device. • Not yet known—E-LMI is still waiting to receive the status from CFM. This condition should not persist for more than a few seconds. • Partially Active—One or more of the remote UNIs is unreachable or down.
EVC Type:	Type of the EVC, with the following possible values: "Point-to-Point," "Multipoint-to-Multipoint," or "EVC type not yet known."

Field	Description
OAM Protocol:	The OAM protocol from which the EVC status and type are derived. Possible values are either "CFM" or "None."
CFM Domain:	Name of the CFM domain for this EVC.
CFM Service:	Name of the CFM service for this EVC.
Remote UNI Count: Configured = *x*, Active = *y*	Number of configured or expected remote UNIs (*x*) and the number of active remote UNIs (*y*) within the EVC.
Remote UNI Id:	ID of each remote UNI, including both configured and active remote UNIs where these two sets are not identical. If the number of configured and active remote UNIs is zero, no table is displayed. **Note** Where no ID is configured for a remote UNI using the **ethernet uni id** command, then the CFM remote MEP ID is displayed, for example, "<Remote UNI Reference Id: *x*>"
Status	Status of each remote UNI, with the following possible values: "Up," "Down," "Admin Down," "Unreachable (a configured remote UNI is not active or missing)," or "Unknown (a remote UNI is active but not reporting its status)."

show ethernet loopback

To display Ethernet data plane loopback information on an interface, use the **show ethernet loopback** command in EXEC mode.

show ethernet loopback [**active** | **permitted**]

Syntax Description

active	Display the details of the active loopback session.
permitted	Displays information on interfaces permitted to run Ethernet loopback.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Task ID

Task ID	Operations
l2vpn	read, write

The following example displays the loopback capabilities per interface.:

```
RP/0/RSP0/CPU0:router# show ethernet loopback permitted

------------------------------------------------------------------------------
Interface                                Dot1q(s)                      Direction
------------------------------------------------------------------------------
tenGigE 0/0/0/1.1                         100                            Internal
tenGigE 0/0/0/0.1                         100                            External
------------------------------------------------------------------------------


/* This example shows all active sessions on the router */

RP/0/RSP0/CPU0:router# show ethernet loopback active
Thu Jul 20 11:00:57.864 UTC
Local: TenGigE0/0/0/0.1, ID 1
============================================
Direction:                           External
Time out:                                None
Time left:                                  -
Status:                                Active
Filters:
  Dot1Q:                                  Any
  Second-dot1Q:                           Any
```

```
  Source MAC Address:                    Any
  Destination MAC Address:               Any
  Class of Service:                      Any
Local: TenGigE0/0/0/0.1, ID 2
=============================================
Direction:                            External
Time out:                                 None
Time left:                                   -
Status:                                 Active
Filters:
  Dot1Q:                                 Any
  Second-dot1Q:                          Any
  Source MAC Address:          0000.0000.0001
  Destination MAC Address:     0000.0000.0002
  Class of Service:                         5
```

Virtual LAN Commands

This section describes the commands used to configure virtual LANs in 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 Virtual LANs in Layer 2 VPNs 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*.

encapsulation default

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

encapsulation default

Syntax Description

This command has no keywords or arguments.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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

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

Only one encapsulation command must be configured per service instance.

Examples

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

```
Router(config-if)# encapsulation default
```

Related Commands

Command	Description
encapsulation dot1q, on page 32	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1ad dot1q, on page 38	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 36	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.

encapsulation dot1q

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

encapsulation dot1q { **any** | *vlan-id* [,*vlan-id* [*-vlan-id*]] } **second-dot1q** *vlan-id*
no encapsulation dot1q { **any** | *vlan-id* [,*vlan-id* [*-vlan-id*]] } **second-dot1q** *vlan-id*

Syntax Description

vlan-id	VLAN ID, can be given as single ID. From Release 6.6.2 onwards, VLAN ID can be given as ranges also.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.
Release 6.6.2	VLAN ID ranges are introduced for inner and outer VLAN tags.

Usage Guidelines

Only one encapsulation statement can be applied to a sub-interface. Encapsulation statements cannot be applied to main interfaces.

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

Examples

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

```
Router(config-if)# encapsulation dot1q 10
```

The following example shows how to map 802.1Q frames ingress on an l2transport sub-interface:

```
Router# configure
Router(config)# interface TenGigE 0/1/0/3.10 l2transport
Router(config-subif)# encapsulation dot1q 10
```

Related Commands

Command	Description
encapsulation dot1q second-dot1q, on page 36	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1ad, on page 34	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.

Command	Description
rewrite ingress tag, on page 43	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.
dot1q tunneling ethertype, on page 3	Configures the Ethertype, used by peer devices when implementing QinQ VLAN tagging, to be 0x9100.

encapsulation dot1ad

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

encapsulation dot1ad *vlan-id* [{**second-dot1ad** *vlan-id*}]
no encapsulation dot1ad

Syntax Description

vlan-id	VLAN ID, can be given as single ID.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Only one encapsulation statement can be applied to a sub-interface. Encapsulation statements cannot be applied to main interfaces.

A single encapsulation dot1ad statement specifies matching for frames with a single VLAN ID.

Examples

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

```
Router(config-if)# encapsulation dot1ad 10
```

The following example shows how to map 802.1ad frames ingress on an l2transport sub-interface:

```
Router# configure
Router(config)# interface TenGigE 0/1/0/3.10 l2transport
Router(config-subif)# encapsulation dot1ad 10
```

Related Commands

Command	Description
encapsulation dot1q second-dot1q, on page 36	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1q, on page 32	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
rewrite ingress tag, on page 43	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.

Command	Description
dot1q tunneling ethertype, on page 3	Configures the Ethertype, used by peer devices when implementing QinQ VLAN tagging, to be 0x9100.

encapsulation dot1q second-dot1q

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

encapsulation dot1q {**any** | *vlan-id* [,*vlan-id* [-*vlan-id*]]} **second-dot1q** *vlan-id* [,*vlan-id* [-*vlan-id*]]
no encapsulation dot1q {**any** | *vlan-id* [,*vlan-id* [-*vlan-id*]]} **second-dot1q** *vlan-id* [,*vlan-id* [-*vlan-id*]]

Syntax Description

vlan-id	VLAN ID, can be given as single ID. From Release 6.6.2 onwards, VLAN ID can be given as ranges also.
second-dot1q	(Optional) Specifies IEEE 802.1Q VLAN tagged packets.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.
Release 6.6.2	VLAN ID ranges are introduced for inner and outer VLAN tags.

Usage Guidelines

The following restrictions are applicable for this command:

- The outer tag must be unique and the inner tag may be a single VLAN.
- QinQ service instance, allows single or multiple on second-dot1q.
- Only one encapsulation command must be configured per service instance.
- Overlapping inner VLAN ranges are not supported.
- VLAN ID ranges cannot be used for both outer and inner tags, simultaneously.

  For example:

  encaps dot1q 10-20 second-dot1q 30-40, is not allowed.

  But either **dot1q 10-20 second-dot1q 30** or **dot1q 10 second-dot1q 30-40** is allowed.

Examples

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

```
Router(config-if)# encapsulation dot1q 10 second-dot1q 20
```

The following example shows how to map ingress frames to a service instance, using VLAN ID ranges:

```
Router(config-if)# encapsulation dot1q 10-20 second-dot1q 30
```

Related Commands

Command	Description
encapsulation dot1q, on page 32	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1ad, on page 34	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.
rewrite ingress tag, on page 43	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.
dot1q tunneling ethertype, on page 3	Configures the Ethertype, used by peer devices when implementing QinQ VLAN tagging, to be 0x9100.

encapsulation dot1ad dot1q

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

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

Syntax Description

dot1ad	Indicates that the IEEE 802.1ad provider bridges encapsulation type is used for the outer tag.
dot1q	Indicates that the IEEE 802.1q standard encapsulation type is used for the inner tag.
vlan-id	VLAN ID, can be given as single ID.

Command Default

No matching criteria are defined.

Command Modes

Sub-interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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

Some of the fields in the 802.1ad VLAN header are interpreted differently per 802.1ad standard.

A **tunneling ethertype** command applied to the main interface does not apply to an 802.1ad sub-interface. An interface with encapsulation dot1ad causes the router to categorize the interface as an 802.1ad interface. This causes special processing for certain protocols and other features:

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

Examples

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

```
Router(config-subif)# encapsulation dot1ad 100 dot1q 20
```

Related Commands

Command	Description
encapsulation dot1q second-dot1q, on page 36	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1ad, on page 34	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.
rewrite ingress tag, on page 43	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.

Command	Description
dot1q tunneling ethertype, on page 3	Configures the Ethertype, used by peer devices when implementing QinQ VLAN tagging, to be 0x9100.

encapsulation list-extended dot1q

To configure up to 64 VLAN-IDs, either on the outer or on the inner VLAN list, use the **encapsulation list-extended dot1q** command in the interface configuration mode. To remove the VLAN-ID configuration, use the **no** form of this command.

encapsulation list-extended dot1q *vlan-id*
no encapsulation list-extended dot1q *vlan-id*

Syntax Description

vlan-id	VLAN ID, can be given as single ID. A comma-separated list of VLAN ranges in the form a-b, c, d, e-f, g and so on.You can configure up to 64 VLAN-IDs.

Command Default

If encapsulation command is not configured, then no matching criteria is defined for that subinterface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

Do not use both the **encapsulation default** and **encapsulation list-extended** commands, on the same subinterface.

- If you migrate from **encapsulation** command to **encapsulation list-extended** command, then **no encapsulation** command must precede the **encapsulation list-extended** command.
- If you migrate from **encapsulation list-extended** command to **encapsulation** command, then **no encapsulation list-extended** command must precede the **encapsulation** command.

The **encapsulation list-extended dot1q** command supports only comma-separated list of outer and inner VLAN tags or VLAN ranges along with untagged Ethernet frames (no spaces allowed between the tags).

Examples

The following example shows how to configure the maximum number of VLAN IDs, on an L2 subinterface:

```
Router(config)#interface TenGigabitEthernet 0/0/0/1.101 l2transport
Router(config-subif)#encapsulation list-extended dot1q
66-67,68-69,70-71,118-119,120-121,122-123,229,230,231
```

encapsulation untagged

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

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

Syntax Description

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

Command Default

No matching criteria are defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

Example 1:

```
Router# configure
Router(config-if)# encapsulation untagged
```

Example 2:

```
Router# configure
```

```
Router(config)# interface GigabitEthernet 0/1/1/0.100 l2transport
Router(config-subif)# encapsulation untagged
```

Related Commands

Command	Description
encapsulation default, on page 31	Configure the default service instance on a port.
encapsulation dot1q, on page 32	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 36	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.

rewrite ingress tag

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

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

Syntax Description

vlan-id	VLAN ID, can be given as single ID.
push dot1q *vlan-id*	Pushes one 802.1Q tag with *vlan-id*.
pop {1}	One tag is removed from the packet. This command can be combined with a push (pop N and subsequent push *vlan-id*).
translate 1-to-1 dot1q *vlan-id*	Replaces the incoming tag (defined in the encapsulation command) into a different 802.1Q tag at the ingress service instance.
translate 1-to-2 dot1q *vlan-id* **dot1q** *vlan-id*	Replaces the incoming tag defined by the encapsulation command by a pair of 802.1Q tags.
translate 2-to-2 dot1q *vlan-id* **second-dot1q** *vlan-id*	Replaces the pair of tags defined by the encapsulation command by a pair of VLANs defined by this rewrite.
symmetric	(Optional) A rewrite operation is applied on both ingress and egress. The operation on egress is the inverse operation as ingress. **Note** Symmetric is the default behavior. Hence, it cannot be disabled.

Command Default

The frame is left intact on ingress.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

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

The **pop** command assumes the elements being popped are defined by the encapsulation type.

The **rewrite ingress tag translate**command assume the tags being translated from are defined by the encapsulation type. In the 2-to-1 option, the “2” means 2 tags of a type defined by the **encapsulation** command.

The translation operation requires at least “from” tag in the original packet. If the original packet contains more tags than the ones defined in the “from”, then the operation should be done beginning on the outer tag.

Examples

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

```
Router(config-if)# rewrite ingress tag push dot1q 200
```

Related Commands

Command	Description
encapsulation dot1q, on page 32	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1ad, on page 34	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second-dot1q, on page 36	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation dot1ad dot1q, on page 38	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.
dot1q tunneling ethertype, on page 3	Configures the Ethertype, used by peer devices when implementing QinQ VLAN tagging, to be 0x9100.

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)

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), on page 5	Enables Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode.

Command	Description
encapsulation dot1ad, on page 34	Defines the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance.

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 PPPoE

Command Default

The load-balancing mode is disabled by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

You must reload the affected line card or chassis to enable the load-balancing mode.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to enable the load balance mode for PPPoE traffic:

```
Router# configure
Router(config)# hw-module profile load-balance algorithm pppoe
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
```

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 or 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	Enables threshold based mac secure.
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 supported on physical and bundle AC, PW, and EVPN.

Task ID

Task ID	Operations
l2vpn	Read, write

Examples

This example shows how to enable MAC security 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 47	Configures an attachment circuit.

Command	Description
l2vpn, on page 55	Enters L2VPN configuration mode.
show l2vpn, on page 68	Displays L2VPN information
show l2vpn xconnect, on page 96	Displays brief information on configured cross-connects.
show l2vpn pw-class, on page 99	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 62	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 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.

Command	Description
pw-class (L2VPN), on page 62	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 7: 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 68	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 55	Enters L2VPN configuration mode.

Command	Description
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	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 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	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** | **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.
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
```

Related Commands

Command	Description
l2vpn, on page 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	Displays L2VPN information
show l2vpn database, on page 76	Displays L2VPN database
show l2vpn forwarding message counters, on page 82	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 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	Displays L2VPN information
show l2vpn database, on page 76	Displays L2VPN database
show l2vpn forwarding, on page 79	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 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	Displays L2VPN information
show l2vpn database, on page 76	Displays L2VPN database
show l2vpn forwarding, on page 79	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 8: show l2vpn resource Command Field Descriptions

Field	Description
Memory	Displays memory status.

Related Commands

Command	Description
l2vpn, on page 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	Displays L2VPN information
show l2vpn index, on page 87	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 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	Displays L2VPN information
show l2vpn index, on page 87	Displays statistics about the index manager.

Command	Description
show l2vpn resource, on page 92	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 9: 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 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	Displays L2VPN information
show l2vpn database, on page 76	Displays L2VPN database
show l2vpn pw-class, on page 99	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 10: 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 55	Enters L2VPN configuration mode.
p2p, on page 61	Enters p2p configuration submode to configure point-to-point cross-connects.
pw-class (L2VPN), on page 62	Enters pseudowire class sub-mode to define a pseudowire class template.
show l2vpn, on page 68	Displays L2VPN information
show l2vpn database, on page 76	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
```

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 47	Configures an attachment circuit.
l2vpn, on page 55	Enters L2VPN configuration mode.

Command	Description
show l2vpn, on page 68	Displays L2VPN information
show l2vpn xconnect, on page 96	Displays brief information on configured cross-connects.

EVPN Commands

This section describes the commands used to configure Ethernet VPN (EVPN) 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, configuration tasks, and examples, see the *EVPN Features* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

ac-aware-vlan-bundling

To configure AC-aware VLAN bundling, use the **ac-aware-vlan-bundling** command in the EVPN configuration mode.

ac-aware-vlan-bundling

Syntax Description This command has no keywords or arguments.

Command Default None.

Command Modes EVPN configuration mode

Command History

Release	Modification
Release 6.6.1	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 configure AC-aware VLAN bundling :

```
Router(config)# evpn
Router(config-evpn)# evi 1
Router(config-evpn-instance)# ac-aware-vlan-bundling
Router(config-evpn-instance)# commit
```

access-signal out-of-service

To override the default signal sent to bring down the AC and to transition the interface to Out-of-Service (OOS) state, use the **access-signal out-of-service** command in the EVPN interface configuration mode. To return to the default behavior, use the **no** form of this command.

access-signal out-of-service

Command Default

None

Command Modes

EVPN interface configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Starting from Cisco IOS XR Release 7.10.1, the EVPN port-active configuration supports hot standby where all the main and subinterfaces up in a Standby node. To revert to the previous behavior of transitioning through the OOS state, use this command.

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows how to configure the access signal mode to enable the OOS functionality.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 01.00.01.00.01.09.01.00.09
Router(config-evpn-ac-es)# load-balancing-mode port-active
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# access-signal out-of-service
Router(config-evpn-ac)# commit
```

access-signal

To configure control signaling messages in access circuits, use the **access-signal** command in the EVPN configuration mode.

access-signal [bundle-down | out-of-service]

Syntax Description

bundle-down	Initiates Access Signal Bundle Down.
out-of-service	Initiates Access signal bundle out of service.

Command Default

None.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to configure **access-signal** command in EVPN configuration mode:

```
RP/0/RP0/CPU0:R1#config
RP/0/RP0/CPU0:R1(config)#evpn
RP/0/RP0/CPU0:R1(config-evpn)#interface Bundle-Ether 1
RP/0/RP0/CPU0:R1(config-evpn-ac)#access-signal bundle-down
```

advertise gateway-ip-disable

To disable advertisement of non-zero EVPN gateway IP address, use the **advertise gateway-ip-disable** command in the EVPN address-family configuration mode.

advertise gateway-ip-disable

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

EVPN address-family configuration mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to disable advertisement of non-zero EVPN gateway IP address:

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.10.10.10
Router(config-bgp-nbr)# remote-as 200
Router(config-bgp-nbr)# update-source Loopback 0
Router(config-bgp-nbr)# address-family l2vpn evpn
Router(config-bgp-nbr-af)# advertise gateway-ip-disable
Router(config-bgp-nbr-af)# commit
```

advertise-mac

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

advertise-mac

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EVPN

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

The following example shows how to advertise local MAC.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 1
Router(config-evpn-evi)# bgp
Router(config-evpn-evi-bgp)# route-target import 100:6005
Router(config-evpn-evi-bgp)# route-target export 100:6005
Router(config-evpn-evi-bgp)# exit
Router(config-evpn-evi)# advertise-mac
```

bgp-gateway

To enable BGP gateway monitoring for host tracking on the Bridge-Group Virtual Interface (BVI) and the bridge domain , use the **bgp-gateway** command on the interface configuration mode on the BVI.

bgp-gateway

Syntax Description

This command has no keywords or arguments.

Command Default

BVI does not monitor the status of the BGP gateways.

Command Modes

Host-tracking configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

You must configure the **host-tracking** command before you configure the **bgp-gateway** command.

Task ID

Task ID	Operation
bfd	read, write

Example

The following example shows how to create a BVI interface, enable host tracking, and enable BVI to monitor the status of the BGP gateways:

```
Router#(config)# interface BVI1
Router#(config-if)# host-routing
Router#(config-if)# vrf vrf_1
Router#(config-if)# ipv4 address 10.0.0.1 255.255.0.0
Router#(config-if)# mac-address 0.dc1.dc2
Router#(config-if)# host-tracking
Router#(config-if-host-tracking)# bgp-gateway
```

clear l2route evpn ipv4

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

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

Syntax Description

ipv4*ipv4-address*	Clears the route for the specified IPv4 address.
all	Clears all EVPN MAC-IPv4 routes that are marked as duplicate or permanently frozen.
evi *evi*	Clears EVPN MAC -IPv4 routes for the specified topology only.
frozen-flag	Clears either duplicate or frozen flag for the MAC-IPv4 routes that are identified by the specified options.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

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

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

clear l2route evpn ipv6

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

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

Syntax Description

ipv6 *ipv6-address*	Clears the route for the specified IPv6 address.
all	Clears all EVPN MAC-IPv6 routes that are marked as duplicate or permanently frozen.
evi *evi*	Clears EVPN MAC-IPv6 routes for the specified topology only.
frozen-flag	Clear duplicate or frozen flag for the MAC-IPv6 routes that are identified by the specified options.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

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

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

clear l2route evpn mac

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

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

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

convergence

To enable the switchover of a failed primary link from one PE device to another, use the **convergence** command in the EVPN configuration submode.

convergence { **mac-mobility** | **reroute** | **nexthop-tracking** }

Syntax Description

mac-mobility	Enables the MAC mobility convergence.
reroute	Redirects the unicast traffic to backup peer.
nexthop-tracking	Enables the EVPN procedures to be influenced by BGP nexthop reachability.

Command Default

None

Command Modes

EVPN configuration submode

Command History

Release	Modification
Release 7.3.1	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 enable mac-mobility reconvergence:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# ethernet-segment
Router(config-evpn-es)# load-balancing-mode single-flow-active
Router(config-evpn-es)# convergence mac-mobility
```

This example shows how to redirect the unicast traffic to backup peer.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether100
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 00.00.00.00.00.00.05.01.02
Router(config-evpn-ac-es)# convergence
Router(config-evpn-ac-es-conv)# reroute
```

core-de-isolation

To configure the recovery time for the EVPN core isolation group after the core interfaces recover from a network failure, use the **core-de-isolation** command in the EVPN Timers configuration mode.

core-de-isolation *timer value*

Syntax Description

core-de-isolation *timer value*	Specifies the core isolation group recovery delay timer. The range is from 60 to 300 seconds. The default timer value is 60 seconds.

Command Default

None.

Command Modes

EVPN Timers configuration mode

Command History

Release	Modification
Release 7.6.1	This command was introduced.

Usage Guidelines

When the core links recover, the default recovery delay timer begins. The access interfaces become active after the core-de-isolation timer expires.

Example

This example shows how to configure the recovery time for the EVPN core isolation group.

```
Router# configure
Router(config)# evpn timers
Router(config-evpn-timers)# core-de-isolation 120
Router(config-evpn-timers)# commit
```

cost-out

To bring down all the bundle interfaces belonging to an Ethernet VPN (EVPN) Ethernet segments on a node, use the **cost-out** command in EVPN configuration mode. To bring up the node into service, use the **no** form of this command.

cost-out
no cost-out

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.1.31	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
EVPN	read, write

Examples

The following example shows how to bring up or bring down the bundle Ethernet Segments on a node:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# cost-out
Router(config-evpn)commit

Router# configure
Router(config)# evpn
Router(config-evpn)# no cost-out
Router(config-evpn)commit
```

delete extcommunity evpn-link-bandwidth

To remove an existing extended community set for EVPN link bandwidth from a route policy, use the **delete extcommunity evpn-link-bandwidth** in route-policy configuration mode.

delete extcommunity evpn-link-bandwidth { **all** | *extcommunity-set* }

Syntax Description

all	All the existing extended community set.
extcommunity-set	The extended community set for EVPN link bandwidth. The set is enclosed in parentheses.

Command Default

None.

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
route-policy	read, write

Example

The following example shows how to remove an extended community set for EVPN link bandwidth from a route policy.

```
Router(config)# route-policy evpn-rpl
Router(config-rpl)# delete extcommunity evpn-link-bandwidth all
Router(config-rpl)# end-policy
```

evi

To enter the EVPN EVI configuration mode and configure BGP settings for a bridge domain or EVI, use the **evi** command in the EVPN configuration mode. To return to the EVPN configuration mode, use the **no** form of this command.

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

Syntax Description

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

Command Default

None.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.1.21	This command was introduced.

Usage Guidelines

Use this command to configure static BGP route distinguisher or BGP route target for an EVI.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enter the EVPN EVI configuration mode:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 2
```

evpn

To enter EVPN configuration mode, use the **evpn** command in the global configuration mode. To return to the global configuration mode, use the **no** form of this command.

evpn [{**bgp** | **evi** | **interface** | **timers**}]
no evpn [{**bgp** | **evi** | **interface** | **timers**}]

Syntax Description

bgp	Configures BGP.
evi	Configures Ethernet VPN ID (EVI).
interface	Assigns an interface to EVPN.
timers	Configures global EVPN timers.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.1.21	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 enter the EVPN configuration mode:

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

evpn evi

To configure EVPN instance (EVI) use the **evpn evi** command in the global configuration mode. To remove the configuration, use the **no** form of this command.

evpn evi *evi-id*

Syntax Description

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

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.6.3	This command was introduced.

Usage Guidelines

The EVI is represented by the virtual network identifier (VNI). An EVI represents a VPN on a PE router. It serves the same role of an IP VPN Routing and Forwarding (VRF), and EVIs are assigned to import/export Route Targets. This command configures the EVI and enters the EVPN Instance configuration mode, where you can configure EVPN settings.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to configure EVPN EVI that enters the EVPN Instance configuration mode.

```
Router# configure
Router(config)# evpn evi 10
Router((config-evpn-instance)#
```

evpn evi multicast source-connected

To configure EVPN multicast instance with a locally connected multicast source, use the **evpn evi** *evi-id* **multicast source-connected** command in the Global configuration mode or EVPN instance configuration mode. To remove the configuration, use the **no** form of this command.

evpn evi *evi-id* [**multicast**] [**source-connected**]

Syntax Description

evi-id	Specifies the Ethernet VPN ID to set. The range is from 1 to 65534.
multicast	(Optional) Configures EVPN instance multicast.
source-connected	(Optional) Connects multicast traffic source.

Command Default

None.

Command Modes

Global configuration

EVPN instance configuration mode

Command History

Release	Modification
Release 6.6.3	This command was introduced.
Release 24.1.1	This command is deprecated

Usage Guidelines

This command is used in all-active dual-homed PE scenarios with BVI interfaces and host-routing for EVPN enabled networks.

This command installs an IPv4 or IPv6 host route in the routing table when a locally connected multicast source is available. This ensures that the Protocol Independent Multicast (PIM) has correct Reverse Path Forwarding (RPF) towards the local source and not to the EVPN-injected host route of the other PE.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to configure a multicast instance in global configuration mode.

```
Router# configure
Router(config)# evpn evi 10 multicast source-connected
Router(config)#
```

This example shows how to configure a multicast instance in EVPN Instance configuration mode.

```
Router# configure
Router(config)# evpn evi 10
Router(config-evpn-instance)# multicast source-connected
Router(config-evpn-instance)#
```

ethernet-segment

To enter the EVPN interface ethernet segment configuration mode, use the **ethernet-segment** command in the EVPN interface configuration mode. To disable the Ethernet segment configuration, use the **no** form of this command.

ethernet-segment [{**backbone-source-mac** | **identifier** | **load-balancing-mode** | **service-carving**}]
no ethernet-segment [{**backbone-source-mac** | **identifier** | **load-balancing-mode** | **service-carving**}]

Syntax Description

backbone-source-mac	Specifies Backbone Source MAC.
identifier	Specifies Ethernet Segment Identifier.
load-balancing-mode	Specifies load balancing mode.
service-carving	Specifies service carving.

Command Default

None.

Command Modes

EVPN interface configuration

Command History

Release	Modification
Release 6.1.21	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to enter the EVPN interface ethernet segment configuration mode:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)#
```

ethernet-segment (evpn)

To disable ESI auto-generation value for LACP ESI type 1, use the **ethernet-segment** command in the EVPN configuration mode. To enable ESI auto-generation, use the **no** form of this command.

ethernet-segmenttype 1 auto-generation-disable
no ethernet-segmenttype 1 auto-generation-disable

Syntax Description

type 1	Specifies LACP ESI-auto-generation for ESI type 1.
auto-generation-disable	Disables ESI auto-generation.

Command Default

By default, EVPN auto-generates an ESI value for the bundle interfaces by retrieving LACP information.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

This command allows mLACP to decide to either forward or stop EVPN multipath resolution on remote ESI.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to disable auto-generation ESI type 1:

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

etree leaf

To enable EVPN Ethernet Tree (E-Tree) services on an EVPN Instance VPN ID and enable an EVPN Instance VPN ID as E-Tree leaf, use the **etree leaf** command in the EVPN configuration mode.

etree leaf

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

If a PE is not configured as E-Tree leaf, it is considered as root by default.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to configure EVPN E-Tree leaf:

```
Router(config)# evpn
Router(config-evpn)# evi 1
Router(config-evpn-instance)# etree leaf
Router(config-evpn-instance)# commit
```

etree rt-leaf

To enable EVPN all-active multihoming support with EVPN E-Tree using BGP Route Target (RT) import and export policies, use the **etree rt-leaf** command in the EVPN EVI configuration submode.

etree rt-leaf

no etree rt-leaf

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

EVI configuration submode

Command History

Release	Modification
Release 7.2.1	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 designate EVPN instance as EVPN E-Tree Route-Target leaf site.

```
Router(config)# evpn
Router(config-evpn)# evi 15
Router(config-evpn-instance)# etree
Router(config-evpn-instance-etree)# rt-leaf
```

host ipv4-address duplicate-detection

To enable duplicate detection of host IPv4 address, use the **host ipv4-address duplicate-detection** command in the EVPN configuration mode.

host ipv4-address duplicate-detection [**freeze-time** *freeze-time* | **move-count** *move-count* | **move-interval** *move-interval* | **retry-count** *retry-count* | **infinity** | **reset-freeze-count-interval** *interval*] **disable**

Syntax Description

freeze-time *freeze-time*	Length of time to lock the IPv4 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 IPv4 address. Default is 5.
move-interval *move-interval*	Interval to watch for subsequent MAC moves before freezing the IPv4 address. Default is 180 seconds.
retry-count *retry-count*	Number of times to unfreeze an IPv4 address before freezing it permanently. Default is three times.
infinite	Infinite retry count. Prevents freezing of the duplicate IP address permanently.
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 IPv4 addresses.

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.6.1	This command was introduced.
Release 7.2.1	**infinite** and **reset-freeze-count-interval** keywords were added.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enable duplicate detection of host IPv4 address:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv4-address duplicate-detection
Router(config-evpn-host-ipv4-addr)# move-count 2
Router(config-evpn-host-ipv4-addr)# freeze-time 10
Router(config-evpn-host-ipv4-addr)# retry-count 2
Router(config-evpn-host-ipv4-addr)# commit
```

This example shows how to prevent permanent freezing of duplicate host IPv4 address:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv4-address duplicate-detection
Router(config-evpn-host-ipv4-addr)# retry-count infinity
Router(config-evpn-host-ipv4-addr)# commit
```

This example shows how to reset the interval after which the count of duplicate detection events are permanently frozen.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv4-address duplicate-detection
Router(config-evpn-host-ipv4-addr)# reset-freeze-count-interval 20
Router(config-evpn-host-ipv4-addr)# commit
```

host ipv6-address duplicate-detection

To enable duplicate detection of host IPv6 address, use the **host ipv6-address duplicate-detection** command in the EVPN configuration mode.

host ipv6-address duplicate-detection [**freeze-time** *freeze-time* | **move-count** *move-count* | **move-interval** *move-interval* | **retry-count** *retry-count* | **infinity** | **reset-freeze-count-interval** *interval*] **disable**

Syntax Description

freeze-time *freeze-time*	Length of time to lock the IPv6 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 IPv6 address. Default is 5.
move-interval *move-interval*	Interval to watch for subsequent MAC moves before freezing the IPv6 address. Default is 180 seconds.
retry-count *retry-count*	Number of times to unfreeze an IPv6 address before freezing it permanently. Default is three times.
infinite	Infinite retry count. Prevents freezing of the duplicate IP address permanently.
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 IPv6 addresses.

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.6.1	This command was introduced.
Release 7.2.1	**infinite** and **reset-freeze-count-interval** keywords were added.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enable duplicate detection of host IPv6 address:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv6-address duplicate-detection
Router(config-evpn-host-ipv6-addr)# move-count 2
Router(config-evpn-host-ipv6-addr)# freeze-time 10
Router(config-evpn-host-ipv6-addr)# retry-count 2
Router(config-evpn-host-ipv6-addr)# commit
```

This example shows how to prevent permanent freezing of duplicate host IPv6 address:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv6-address duplicate-detection
Router(config-evpn-host-ipv6-addr)# retry-count infinity
Router(config-evpn-host-ipv6-addr)# commit
```

This example shows how to reset the interval after which the count of duplicate detection events are permanently frozen.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv6-address duplicate-detection
Router(config-evpn-host-ipv6-addr)# reset-freeze-count-interval 20
Router(config-evpn-host-ipv6-addr)# commit
```

evpn-link-bandwidth

To configure EVPN link bandwidth, use the **evpn-link-bandwidth** command in VRF neighbor address family configuration mode.

evpn-link-bandwidth [**per-path** *unit*]

Syntax Description

per-path	(Optional) EVPN link bandwidth uses per path.
unit	Unit value per path. The range is from 1 to 65535.

Command Default

None.

Command Modes

VRF neighbor address family configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
bgp	read, write

Example

The following example shows configuration of EVPN link bandwidth on a VRF neighbor.

```
Router(config)# router bgp 100
Router(config-bgp)# vrf vrf1
Router(config-bgp-vrf)# neighbor 172.16.1.3
Router(config-bgp-vrf-nbr)# evpn-link-bandwidth per-path 100
```

host mac-address duplicate-detection

To enable duplicate detection of host MAC address, use the **host mac-address duplicate-detection** command in the EVPN configuration mode.

host mac-address duplicate-detection [**freeze-time** *freeze-time* | **move-count** *move-count* | **move-interval** *move-interval* | **retry-count** *retry-count* | **infinity** | **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 an MAC address before freezing it permanently. Default is three times.
infinite	Infinite retry count. Prevents freezing of the duplicate MAC address permanently.
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 addresses.

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.6.1	This command was introduced.
Release 7.2.1	**infinite** and **reset-freeze-count-interval** keywords were added.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enable duplicate detection of host MAC address:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host MAC-address duplicate-detection
Router(config-evpn-host-mac-addr-dup-detection)# move-count 2
Router(config-evpn-host-mac-addr-dup-detection)# freeze-time 10
Router(config-evpn-host-mac-addr-dup-detection)# retry-count 2
Router(config-evpn-host-mac-addr-dup-detection)# commit
```

This example shows how to prevent permanent freezing of duplicate host MAC address:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host MAC-address duplicate-detection
Router(config-evpn-host-mac-addr-dup-detection)# retry-count infinity
Router(config-evpn-host-mac-addr-dup-detection)# commit
```

This example shows how to reset the interval after which the count of duplicate detection events are permanently frozen.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# host MAC-address duplicate-detection
Router(config-evpn-host-mac-addr-dup-detection)# reset-freeze-count-interval 20
Router(config-evpn-host-mac-addr-dup-detection)# commit
```

hw-module l2-replication core-optimized

By default, the BUM traffic from the core is replicated not only towards the attachment circuits (AC) but also towards the remote PEs in the Ingress pipeline. The packets replicated towards the remote PEs are dropped in the Egress Pipeline by applying the Split-Horizon rule. Even though these replicated packets get dropped in the Egress Pipeline, it results in recycle bandwidth being utilised.

For optimising the recycle bandwidth utilization, enable the **hw-module l2-replication core-optimized** command in the global configuration mode. Once you enable this command, the BUM traffic received from the core will:

- No longer be replicated to remote PEs in the Ingress pipeline.
- Only be replicated to the attachment circuits.

To return to the default behaviour, use **no hw-module l2-replication core-opitmized**.

hw-module l2-replication core-optimized

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

You must manually reload the router to activate the **hw-module l2-replication core-optimized** command.

Task ID

Task ID	Operation
root-lr	read, write

Example

The following example shows how to enable the command for optimising the recycle bandwidth utilization during the BUM traffic replication from the core.

```
Router# configure
Router(config)# hw-module l2-replication core-optimized
```

host-tracking

To enable host tracking on a Bridged Virtual Interface (BVI), allowing a device to keep track of hosts directly connected to it, use the **host-tracking** command.

host-tracking [*bgp-gateway*]

Syntax Description

bgp-gateway	Specifies that the BVI monitors the status of hosts that are considered to be gateways for BGP and adjusts its behavior based on the availability or reachability of those gateways.

Command Default

Disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

None.

Task ID

Task ID	Operation
bfd	read, write

Example

The following example shows how to create a BVI and enable host tracking:

```
Router#(config)# interface BVI1
Router#(config-if)# host-tracking
Router#(config-if-host-tracking)# bgp-gateway
Router#(config-if-host-tracking)# arp
Router#(config-if-host-tracking-arp)# bfd fast-detect
```

flood mode ac-shg-optimized

To avoid the replication of BUM flood traffic towards attachment circuits (AC) in a split-horizon group (SHG), use the **flood mode ac-shg-optimized** command in the L2VPN bridge group bridge domain configuration mode. To return to the default behavior, use the **no** form of this command.

flood mode ac-shg-optimized

Command Default

None

Command Modes

L2VPN bridge group bridge domain configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

To enable the optimization of AC-to-AC replication of BUM flood traffic, ensure that all the ACs are available in a split-horizon group. In addition, ensure that you have already configured the **hw-module l2-replication core-optimized** command and restarted the router, so that the command takes effect.

Note The **flood mode ac-shg-optimized** command works only after you configure the **hw-module l2-replication core-optimized** command and restart the router.

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows configuration of flood mode optimization, which avoids the AC-to-AC replication of BUM flood traffic.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg0
Router(config-l2vpn-bg)# bridge-domain bd0
Router(config-l2vpn-bg-bd)# flood mode ac-shg-optimized
```

force single-homed

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

force single-homed
no force single-homed

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

All EVPN-based access redundancy (EVLAG) designated forwarder elections are disregarded in favor of the legacy MCLAG access protection protocol.

When CE is directly connected to a PE through a physical or bundle port and the redundant connection to another PE is operating an MCLAG redundancy group.

Specifically, the ESI assignment to the interface is no longer used for EVPN-based access redundancy and protection mechanisms and the MCLAG redundancy protocol will control the state of this interface.

With this command only the access protection is relinquished, and EVPN core mechanisms remain operational including any core functionality requiring the use of an ESI. This command is different than assigning ESI-0 to the interface, and functions also with an assigned ESI. With MCLAG control of the interface state, those EVPN core procedures that depend on interface state remain the same.

Use this command to force the interface into single homed EVPN mode and interoperate with MCLAG access protection.

The following example shows how to configure force single-homed.

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

import from bridge-domain

To import IPv4 or IPv6 host routes from all the EVPN bridge domains in a router, use the **import from bridge-domain** in BGP address family configuration mode. To remove the configuration, use the **no** form of this command.

import from bridge-domain

Command Default

None.

Command Modes

BGP address family configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
bgp	read, write

Example

The following example shows configuration to import IPv4 host routes as IPv4 unicast routes from EVPN bridge domains.

```
Router(config)# router bgp
Router(config-bgp)# address-family ipv4 unicast
Router(config-bgp-af)# import from bridge-domain
```

import from bridge-domain advertise-as-vpn

To import EVPN route type-2 routes from EVI bridge domain into the L3VPN VRF, and advertise as VPNv4 or VPNv6 routes, use the **import from bridge-domain advertise-as-vpn** command in the global configuration mode.

import from bridge-domain advertise-as-vpn

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

The route target of the EVI (BD) must match with at least one import route-target of the L3 VRF.

If the remote node uses BGP VPNv4 or VPNv6 address-family instead of EVPN address-family, use the **import from bridge-domain advertise-as-vpn** command under VRF address-family that allows you to advertise the host-route as BGP VPNv4 or VPNv6 instead of EVPN address-family.

The following example shows how to configure import from bridge-domain advertise-as-vpn.

```
Router# configure
Router(config)# vrf A
Router(config-vrf)# address-family ipv4 unicast
Router(config-vrf-af)# import from bridge-domain advertise-as-vpn
Router(config-vrf-af)# import route-target 30:30
Router(config-vrf-af)# export route-target 30:30
Router(config-vrf-af)# commit
```

implicit-import

To import EVPN routes in BGP routing table, use **implicit-import** command in the EVPN configuration mode.

implicit-import

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to configure **implicit-import** command in EVPN configuration mode.

```
RP/0/RP0/CPU0:R1#config
RP/0/RP0/CPU0:R1(config)#evpn
RP/0/RP0/CPU0:R1(config-evpn)#evi 1
RP/0/RP0/CPU0:R1(config-evpn-instance)#bgp
RP/0/RP0/CPU0:R1(config-evpn-instance-bgp)#implicit-import
```

interface (EVPN)

To enter the physical port interface or the bundle name interface configuration mode, use the **interface** command in the EVPN configuration mode. To return to the EVPN configuration mode, use the **no** form of this command.

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

Syntax Description

type	Specifies the physical ethernet interface or bundle ethernet Interface type connected to the CE device. For more information about the syntax for the router, use the question mark (**?**) online help function.
interface path-id	Physical port name or main bundle name. The range for the bundle name is from 1 to 65535. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

None.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.1.21	This command was introduced.

Usage Guidelines

To specify a physical interface, the notation for the *interface-path-id* is *rack/slot/module/port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:

- *rack*: Chassis number of the rack.
- *slot*: Physical slot number of the line card.
- *module*: Module number. A physical layer interface module (PLIM) is always 0.
- *port*: Physical port number of the interface.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enter the EVPN Interface configuration mode for bundle-ether 1:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)#
```

l2vpn evpn

To execute EVPN commands in L2VPN mode, use the **l2vpn evpn** command in the EXEC mode.

l2vpn evpn { **compute-hrw neighbor** *neighbor-ip-address* **esi** *esi-value* **service-id** *evi-value* | **ethernet-segment interface** *interface-name* **revert** }

Syntax Description

compute-hrw neighbor *neighbor-ip-address* **esi** *esi-value* **service-id***evi-value*	Generates Highest Random Weight (HRW) for a PE, which would be used during the DF election.
ethernet-segment interface *interface-name* **revert**	Disables the non-revertive mode and returns to the revertive mode of DF election.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.0.1	This command was introduced.
Release 24.1.1	The **ethernet-segment interface** *interface-name* **revert** keyword was added.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows configuration to compute HRW.

```
Router# l2vpn evpn compute-hrw neighbor 10.1.1.1 esi 11.1111.1111.0011.1111 service-id 10
```

This example shows configuration to disable the non-revertive mode of DF election.

```
Router# l2vpn evpn ethernet-segment interface Bundle-Ether1 revert
```

load-balancing-mode

To enable the load-balancing mode, use the **load-balancing-mode** command in the EVPN interface configuration mode. To disable the load-balancing mode, use the **no** form of this command.

load-balancing-mode { **port-active** | **single-active** | **single-flow-active** }

Syntax Description

port-active	Enables the port-active load-balancing mode
single-active	Enables the single-active load-balancing mode.
single-flow-active	Enables the single-flow-active load-balancing mode.

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.
Release 7.1.15	Port-active keyword was added.
Release 7.3.1	single-flow-active keyword was added.

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 enable the single-active load-balancing mode:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# ethernet-segment
Router(config-evpn-es)# load-balancing-mode single-active
```

This example shows how to enable the single-flow-active load-balancing mode:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# ethernet-segment
Router(config-evpn-es)# load-balancing-mode single-flow-active
```

mac-flush

To perform a MAC flush on an Ethernet-segment, use the **mac-flush** command in the EVPN interface configuration mode. To disable the MAC flush setting, use the **no** form of this command.

mac-flush mvrp

Starting from Cisco IOS XR Release 7.11.2, the command has been replaced as follows:

mac-flush-message { **mvrp** | **disable** }

Syntax Description

mvrp	Specifies the MAC flush over MVRP.
disable	Disables the MAC flush messages.

Command Default

STP-TCN

Command Modes

EVPN interface configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.
Release 7.11.2	This command was replaced by the **mac-flush-message** command. The keyword **disable** was added.

Usage Guidelines

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

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to perform the MAC flush over MVRP on an Ethernet segment:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 36.37.00.00.00.00.00.11.00
Router(config-evpn-ac-es)#exit
Router(config-evpn-ac)# mac-flush mvrp
Router(config-evpn-ac)#
```

This example shows how to perform the MAC flush over MVRP on an Ethernet segment, starting from release 7.11.2:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 36.37.00.00.00.00.00.11.00
Router(config-evpn-ac-es)#exit
Router(config-evpn-ac)# mac-flush-message mvrp
Router(config-evpn-ac)#
```

This example shows how to disable the MAC flush messages on an Ethernet segment:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 36.37.00.00.00.00.00.11.00
Router(config-evpn-ac-es)#load-balancing-mode single-active
Router(config-evpn-ac-es)#exit
Router(config-evpn-ac)# mac-flush-message disable
Router(config-evpn-ac)#
```

neighbor evpn

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

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

Syntax Description

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

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 6.1.21	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

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

```
Router# configurerouter# interface TenGigE0/1/0/12
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group xc1
Router(config-l2vpn-xc)# p2p vpws
Router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 100 target 80
```

non-revertive

To enable the non-revertive mode of DF election, use the **non-revertive** command in the EVPN ethernet segment service carving configuration mode.

non-revertive

Command Default

None

Command Modes

EVPN interface Ethernet segment service carving configuration mode

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

You can enable the non-revertive mode only on preference-based DF election. It is recommended to configure the non-revertive mode on all the nodes in the network.

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to enable non-revertive mode:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 01.11.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode port-active
Router(config-evpn-ac-es)# service-carving preference-based
Router(config-evpn-ac-es-sc-pref)# non-revertive
Router(config-evpn-ac-es-sc-pref)# weight 100
Router(config-evpn-ac-es-sc-pref)# commit
```

option-b-asbr-only

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

option-b-asbr-only

Syntax Description

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

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

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

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

preferred-nexthop

To choose a particular remote PE in a dual-homed mode to be the nexthop, use the **preferred-nexthop** command in the EVPN configuration submode.

preferred-nexthop [{ **highest-ip** | **lowest-ip** | **modulo** }]

Syntax Description

highest-ip	Selects the highest IP address as the primary nexthop.
lowest-ip	Selects the lowest IP address as the primary nexthop.
modulo	Determines which remote is primary using the formula EVI % 2.

Command Default

None

Command Modes

EVPN configuration submode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to configure the highest IP address as the primary nexthop.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 100
Router(config-evpn-evi)# preferred-nexthop highest-ip
Router(config-evpn-evi)# commit
```

This example shows how to configure the lowest IP address as the backup nexthop.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 100
Router(config-evpn-evi)# preferred-nexthop lowest-ip
Router(config-evpn-evi)# commit
```

This example shows how to configure the primary nexthop using the modulo keyword.

```
Router# configure
```

```
Router(config)# evpn
Router(config-evpn)# evi 100
Router(config-evpn-evi)# preferred-nexthop modulo
Router(config-evpn-evi)# commit
```

revert

To set a timer to switchover from non-revertive mode to revertive mode of DF election, use the **revert** *timer* command in the EVPN configuration mode or EVPN interface configuration mode.

revert *timer*

Syntax Description

timer	Specify the time interval for the revert timer in seconds. The range is 0 to 3600.

Command Default

None

Command Modes

- EVPN configuration mode
- EVPN interface configuration mode

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows revert timer configuration for a specific interface:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 01.11.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode port-active
Router(config-evpn-ac-es)# service-carving preference-based
Router(config-evpn-ac-es-sc-pref)# non-revertive
Router(config-evpn-ac-es-sc-pref)# weight 100
Router(config-evpn-ac-es-sc-pref)# exit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# timers
Router(config-evpn-ac-timers)# revert 300
Router(config-evpn-ac-es)# commit
```

This example shows global configuration for revert timer:

```
Router# configure
```

```
Router(config)# evpn
Router(config-evpn)# timers
Router(config-evpn-timers)# revert 300
Router(config-evpn-timers)# commit
```

route-target

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

route-target {*as-number:nn ip-address:nn* }
no route-target {*as-number:nn ip-address:nn* }

Syntax Description

as-number:nn Autonomous system (AS) number of the route distinguisher.

- as-number—16-bit AS number

  Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535.

- nn—32-bit number

ip-address:nn IP address of the route distinguisher.

- ip-address—32-bit IP address
- nn—16-bit number

Command Default

None.

Command History

Task ID

Task ID	Operations
l2vpn	read, write

Examples

service-carving

To specify a list of service identifiers as active and standby services, use the **service-carving** command in the EVPN Ethernet segment configuration mode.

service-carving { **manual** [**primary** *service-id-range* **secondary** *service-id-range*] } | { **preference-based** [**access-driven** | **weight** *preference-df-weight* }]

Syntax Description

manual	Specifies service identifiers or EVI-list services manually.
primary	Specifies the primary services list.
secondary	Specifies the secondary services list.
service-id-range	Specifies the services list notation in the range 100, 201-300, 401. The range is within 256 to 16777214.
preference-based	Specifies preference-based service carving.
access-driven	Specifies acess-driven DF election.
weight	Specifies the preference value.
preference-df-weight	Specifies the preference DF weight. The range is from 0 to 65535 unless **access-driven** is configured, in which case it will be 0 to 32767. Default is 32767 when not configured.

Command Default

Automatic service carving

Command Modes

EVPN interface Ethernet segment configuration mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.
Release 7.3.1	The follwing keywords are added: • **preference-based** • **access-driven**

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

This example shows how to specify a list of service identifiers as active and standby services:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-ether 1
Router(config-evpn-ac)# ethernet segment
Router(config-evpn-ac-es)# service-carving manual primary 201-300 secondary 400-500
Router(config-evpn-ac-es)# commit
```

Example

This example shows how to sepcify EVPN access-driven DF election:

```
Router#configure
Router(config)#evpn
Router(config-evpn)#interface Bundle-Ether1
Router(config-evpn-ac)#ethernet-segment
Router(config-evpn-ac-es)#identifier type 0 01.11.00.00.00.00.00.00.01
Router(config-evpn-ac-es)#load-balancing-mode port-active
Router(config-evpn-ac-es)#service-carving preference-based
Router(config-evpn-ac-es-sc-pref)#weight 100
Router(config-evpn-ac-es-sc-pref)#access-driven
Router(config-evpn-ac-es-sc-pref)#commit
```

set advertise-evpn-gw-ip

To advertise the EVPN gateway IP address as a next-hop IP address,, use the **set advertise-evpn-gw-ip** command in the route-policy configuration mode.

set advertise-evpn-gw-ip { **A.B.C.D** | **X:X::X** | **parameter** | **use-next-hop** }

Syntax Description

A.B.C.D	Specify an IPv4 address.
X:X::X	Specify an IPv6 address.
parameter	Identifier specified in the format: '$' followed by alphanumeric. characters
use-next-hop	Set advertise EVPN gateway IP as next-hop IP address.

Command Default

None

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
route-policy	read, write

Example

This example shows how to configure EVPN gateway IP address as a next-hop IP address:

```
Router(config)# route-policy gw
Router(config-rpl)# set advertise-evpn-gw-ip use-next-hop
Router(config-rpl)# end-policy
Router(config)# vrf VRF1
Router(config-vrf)# address-family ipv4 unicast
Router(config-vrf-af)# import route-target
Router(config-vrf-import-rt)# 10:10
Router(config-vrf-import-rt)# exit
Router(config-vrf-af)# export route-policy gw
Router(config-vrf-af)# export route-target
Router(config-vrf-export-rt)# 10:10
Router(config-vrf-export-rt)#commit
```

set extcommunity evpn-link-bandwidth

To set the extended community attribute for EVPN link bandwidth, use the **set extcommunity evpn-link-bandwidth** in route-policy configuration mode.

set extcommunity evpn-link-bandwidth { *extcommunity-set* | *parameter* }

Syntax Description

extcommunity-set	The extended community set for EVPN link bandwidth. The set is enclosed in parentheses.
parameter	Parameter name. The parameter name must be preceded by a "$."

Command Default

None.

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
route-policy	read, write

Example

The following example shows how to set the extended community attribute for EVPN link bandwidth using an extended community set.

```
Router(config)# route-policy evpn-rpl
Router(config-rpl)# set extcommunity evpn-link-bandwidth (1 : 8000)
Router(config-rpl)# end-policy
```

show bgp l2vpn evpn

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

show bgp l2vpn evpn {**bridge-domain** *bridge-domain-name* | **rd** { **all** *IPv4 address:nn* *4-byte as-number:nn* *2-byte as-number:nn* } | **gateway-track** { **interface BVI identifier** | **standby** } }

Syntax Description

bridge-domain *bridge-domain-name*	Displays the bridges by the bridge ID. The bridge-domain-name argument is used to name a bridge domain.
rd	Displays routes with specific route distinguisher.
all	Displays specified routes in all RDs.
IPv4 address:nn	Specifies the IPv4 address of the route distinguisher. nn: 16-bit number
4-byte as-number:nn	Specifies 4-byte AS number in asdot (X.Y) format or in asplain format. • For 4-byte AS number in asdot (X.Y) format, the range is from 1 to 65535. The format is: <1-65535>.<0-65535>:<0-65535> • For 4-byte AS number in asplain format, the range is from 65536 to 4294967295. The format is: <65536-4294967295>: nn: 32-bit number
2-byte as-number:nn	Specifies 2-byte as-number. The range is from 1 to 65535. nn: 32-bit number
gateway-track	Displays tracking status of the EVPN gateways.
interface	Displays the interface.
BVI	Displays the Bridge-Group Virtual Interface (BVI).
identifier	BVI Identifier
standby	Displays information related to standby gateways.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.21	This command was introduced.

Release	Modification
Release 7.11.1	The control word and flow label signaling attributes were added.
Release 24.1.1	This command was modified. The keywords: **gateway-track** , **interface**, **BVI** *identifier*, and **standby** were added.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
bgp	read

Example

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

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

Example

The following sample output displays the control word and flow label signaling attributes. Mismatch in EVPN L2 attributes between the local and remote nodes can impact the EVPN-VPWS PW or E-LAN service.

The following table describes the EVPN L2 attributes.

EVPN L2 Attributes	Description
0x01	Indicates that the PE functions a backup router.
0x02	Indicates that the PE functions as a primary router.

EVPN L2 Attributes	Description
0x04	Indicates that the control word is enabled and flow label signalling is disabled on the PE.
0x08	Indicates that the flow label signalling is enabled and control word is disabled on the PE.

The following output indicates that the control word is enabled and flow label signalling is disabled on the PE.

```
Router# show bgp l2vpn evpn rd 192.168.10.1:2705 [3][0][32][192.168.10.1]/80 detail
BGP routing table entry for [3][0][32][192.168.10.1]/80, Route Distinguisher:
192.168.10.1:2705
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker              286721       286721
    Flags: 0x00140001+0x00000000;
Paths: (1 available, best #1)
  Advertised to update-groups (with more than one peer):
    0.2
  Path #1: Received by speaker 0
  Flags: 0x202000000504000b+0x00, import: 0x000, EVPN: 0x0
  Advertised to update-groups (with more than one peer):
    0.2
  Local
    0.0.0.0 from 0.0.0.0 (192.168.1.1), if-handle 0x00000000
      Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate
      Received Path ID 0, Local Path ID 1, version 286721
      Extended community: EVPN L2 ATTRS:0x04:0 RT:64600:2705
      IMET PMSI Originator Nexthop Address : 192.168.10.1 (reachable)
      PMSI: flags 0x00, type 6, label 24004, ID 0xc0a80a01
```

The following output indicates that the EVPN gateway is enabled. The output displays the interface identifier, the bridge associated with the interface, and the VRF instance associated with the interface.

```
Router# show bgp l2vpn evpn gateway-track interface BVI 1
Interface       Bridge                VRF
BVI1            evpn1                 vrf1
```

show evpn ethernet-segment

To display the EVPN Ethernet segment information, use the **show evpn ethernet-segment** command in the EXEC mode.

show evpn ethernet-segment [{ **detail** | **esi** | **interface** | **location** | **private** | **standby** | **carving** }]

Syntax Description

detail	Displays detailed information.
esi	Filters by Ethernet Segment identifier.
interface	Filters by interface name.
location	Displays location specific information.
private	Displays private information.
standby	Displays standby node specific information.
carving	Filters by carving details.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.21	This command was introduced.
Release 7.3.1	The **carving** keyword was added.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN Ethernet segment detailed information:

```
Router#show evpn ethernet-segment detail
Tue Jun 25 14:17:09.610 EDT
Legend:
  A- PBB-EVPN load-balancing mode and Access Protection incompatible,
  B- no Bridge Ports PBB-EVPN enabled,
  C- Backbone Source MAC missing,
```

```
  E- ESI missing,
  H- Interface handle missing,
  I- Interface name missing,
  M- Interface in Down state,
  O- BGP End of Download missing,
  P- Interface already Access Protected,
  Pf-Interface forced single-homed,
  R- BGP RID not received,
  S- Interface in redundancy standby state,
  X- ESI-extracted MAC Conflict

Ethernet Segment Id      Interface      Nexthops
------------------------ -------------- ----------------------------------------
0210.0300.9e00.0210.0000 Gi0/3/0/0      1.100.100.100
                                        2.100.100.100
  ES to BGP Gates   : Ready
  ES to L2FIB Gates : Ready
  Main port         :
     Interface name : GigabitEthernet0/3/0/0
     IfHandle       : 0x1800300
     State          : Up
     Redundancy     : Not Defined
  Source MAC        : 0001.ed9e.0001 (PBB BSA)
  Topology          :
     Operational    : MHN
     Configured     : A/A per service (default)
  Primary Services  : Auto-selection
  Secondary Services: Auto-selection
  Service Carving Results:
     Bridge ports   : 3
     Elected        : 0
     Not Elected    : 3
          I-Sid NE  :  1450101, 1650205, 1850309
  MAC Flushing mode : STP-TCN
  Peering timer     : 45 sec [not running]
  Recovery timer    : 20 sec [not running]
  Flushagain timer  : 60 sec

be01.0300.be01.ce00.0001 BE1            1.100.100.100
                                        2.100.100.100
  ES to BGP Gates   : Ready
  ES to L2FIB Gates : Ready
  Main port         :
     Interface name : Bundle-Ether1
     IfHandle       : 0x000480
     State          : Up
     Redundancy     : Active
  Source MAC        : 0024.be01.ce00 (Local)
  Topology          :
     Operational    : MHN
     Configured     : A/A per flow (default)
  Primary Services  : Auto-selection
  Secondary Services: Auto-selection
  Service Carving Results:
     Bridge ports   : 3
     Elected        : 3
          I-Sid E   :  1450102, 1650206, 1850310
     Not Elected    : 0
  MAC Flushing mode : STP-TCN
  Peering timer     : 45 sec [not running]
  Recovery timer    : 20 sec [not running]
  Flushagain timer  : 60 sec
```

This sample output shows the EVPN Ethernet segment carving detailed information with Single-Flow-Active mode enabled.

```
Router# show evpn ethernet-segment carving detail
Thu Aug  6 13:00:37.988 IST
Legend:
  B   - No Forwarders EVPN-enabled,
  C   - Backbone Source MAC missing (PBB-EVPN),
  RT  - ES-Import Route Target missing,
  E   - ESI missing,
  H   - Interface handle missing,
  I   - Name (Interface or Virtual Access) missing,
  M   - Interface in Down state,
  O   - BGP End of Download missing,
  P   - Interface already Access Protected,
  Pf  - Interface forced single-homed,
  R   - BGP RID not received,
  S   - Interface in redundancy standby state,
  X   - ESI-extracted MAC Conflict
  SHG - No local split-horizon-group label allocated

Ethernet Segment Id      Interface                         Nexthops
------------------------ --------------------------------- --------------------
0000.0000.0000.0000.0001 BE1                               10.0.0.1
                                                           172.16.0.1
  ES to BGP Gates   : Ready
  ES to L2FIB Gates : Ready
  Main port         :
     Interface name : Bundle-Ether1
     Interface MAC  : 008a.96ee.88dc
     IfHandle       : 0x20005f5c
     State          : Up
     Redundancy     : Not Defined
  ESI type          : 0
     Value          : 00.0000.0000.0000.0001
  ES Import RT      : 0000.0000.0001 (Local)
  Source MAC        : 0000.0000.0000 (N/A)
  Topology          :
     Operational    : MH, Single-flow-active
     Configured     : Single-flow-active
  Service Carving   : Auto-selection
     Multicast      : Disabled
  Convergence       : MAC-Mobility,
     Mobility-Flush : Debounce 13 sec, Count 1, Skip 1499
                    : Last 01/01 05:57:42.468
  Peering Details   : 2 Nexthops
  10.0.0.1[MOD:P:00:T]
    172.16.0.1 [MOD:P:7fff:T]
  Service Carving Synchronization:
     Mode           : NONE
     Peer Updates   :
  Service Carving Results:
     Forwarders     : 1000
     Elected        : 1000
            EVI E   :        1,       2,       3,       4,       5,       6
            EVI E   :        7,       8,       9,      10,      11,      12,
            EVI E   :       13,      14,      15,      16,      17,      18,
            EVI E   :       19,      20,      21,      22,      23,      24,
[........]
            EVI E   :      979,     980,     981,     982,     983,     984,
            EVI E   :      985,     986,     987,     988,     989,     990,
            EVI E   :      991,     992,     993,     994,     995,     996,
            EVI E   :      997,     998,     999,    1000
     Not Elected    : 0
```

```
EVPN-VPWS Service Carving Results:
   Primary        : 0
   Backup         : 0
   Non-DF         : 0
MAC Flushing mode : STP-TCN
Peering timer     : 3 sec [not running]
Recovery timer    : 30 sec [not running]
Carving timer     : 0 sec [not running]
Local SHG label   : 29096
Remote SHG labels : 1
            29096 : nexthop 10.0.0.1
Access signal mode: Bundle OOS (Default)
```

show evpn evi

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

show evpn evi [{**bridge-domain** | **detail** | **inclusive-multicast** | **location** | **mac** | **standby** | **vpn-id** }]

Syntax Description

bridge-domain	Displays information for a specified bridge-domain..
detail	Displays detailed information.
inclusive-multicast	Displays EVPN Inclusive Multicast information.
location	Displays location specific information.
mac	Displays EVI MAC route associated configuration information.
standby	Displays standby node specific information.
vpn-id	Displays information for a specified E-VPN Identifier.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.21	This command was introduced.
Release 7.11.1	The control word and flow label signaling attributes were added.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN EVI information with the VPN-ID and MAC address filter:

```
Router#show evpn evi vpn-id 185 mac 0024.be03.ce01
MAC address    Nexthop                                 Label    vpn-id
-------------- --------------------------------------- -------- --------
0024.be03.ce01 3.100.100.100                           16004    185
               4.100.100.100                           16004    185
   ESI port key : 0x0000
   Source       : Remote
```

```
   Flush Count  : 0
```

This sample output shows the EVPN EVI information with the VPN-ID and inclusive-multicast filter:

```
Router#show evpn evi vpn-id 185 inclusive-multicast service-id 1850312 orig-ip 1.100.100.100
ISID          Originating IP                vpn-id
------------- ----------------------------- ----------
1850312       1.100.100.100                           185
1850312       2.100.100.100                           185
1850312       3.100.100.100                           185
1850312       4.100.100.100                           185
```

This sample output shows the EVPN EVI inclusive-multicast information:

```
Router#show evpn evi inclusive-multicast detail
ISID: 1850312, Originating IP: 1.100.100.100                          185
    Nexthop: ::
    Label  : 16005
    Source : Local
ISID: 1850312, Originating IP: 2.100.100.100                          185
    Nexthop: 2.100.100.100
    Label  : 16005
    Source : Remote
ISID: 1850312, Originating IP: 3.100.100.100                          185
    Nexthop: 3.100.100.100
    Label  : 16005
    Source : Remote
ISID: 1850312, Originating IP: 4.100.100.100                          185
    Nexthop: 4.100.100.100
    Label  : 16005
    Source : Remote
```

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

```
Router#show evpn evi bridge-domain tb1-core1 detail
EVI        Bridge Domain                Type
---------- ---------------------------- -------
145        tb1-core1                    PBB
165        tb1-core2                    PBB
185        tb1-core3                    PBB
65535      ES:GLOBAL                    BD
```

This sample output shows the EVPN EVI detailed information:

```
Router#show evpn evi detail
EVI        Bridge Domain                Type
---------- ---------------------------- -------
145        tb1-core1                    PBB
   Unicast Label  : 16000
   Multicast Label: 16001
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:145
   RT Auto  : 100:145
   Route Targets in Use           Type
   ------------------------------ -------
   100:145                        Import
   100:145                        Export
```

```
165        tb1-core2                    PBB
   Unicast Label  : 16002
   Multicast Label: 16003
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:165
   RT Auto  : 100:165
   Route Targets in Use           Type
   ------------------------------ -------
   100:165                        Import
   100:165                        Export

185        tb1-core3                    PBB
   Unicast Label  : 16004
   Multicast Label: 16005
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:185
   RT Auto  : 100:185
   Route Targets in Use           Type
   ------------------------------ -------
   100:185                        Import
   100:185                        Export

65535      ES:GLOBAL                    BD
   Unicast Label  : 0
   Multicast Label: 0
   RD Config: none
   RD Auto  : (auto) 1.100.100.100:0
   RT Auto  : none
   Route Targets in Use           Type
   ------------------------------ -------
   0100.9e00.0210                 Import
   0100.be01.ce00                 Import
   0100.be02.0101                 Import
```

Example

The following sample output displays the control word and flow label signaling attributes. The output shows whether the control word and flow label signaling are locally enabled.

```
Router# show evpn evi vpn-id 2705 inclusive-multicast detail
VPN-ID     Encap  EtherTag   Originating IP
---------- ------ ---------- ---------------------------------------
2705       MPLS   0          192.168.10.1
    TEPid  : 0xffffffff
    PMSI Type: 6
    Nexthop: ::
    Label  : 24004
    SR-TE Info: N/A
    Source : Local
    E-Tree : Root
    Layer 2 Attributes:
     DF Role : Not Specified
     CW      : Disabled
     FL      : Disabled
     MTU     : 0
     Sig DF  : Not Specified
2705       MPLS   0          192.168.20.1
    TEPid  : 0x02000002
    PMSI Type: 6
    Nexthop: 192.168.20.1
```

```
    Label  : 24004
    SR-TE Info: N/A
    Source : Remote
    E-Tree : Root
    Layer 2 Attributes:
     DF Role : NDF
     CW      : Disabled
     FL      : Disabled
     MTU     : 0
     Sig DF  : NDF
2705       MPLS   0          192.168.30.1
    TEPid  : 0x02000001
    PMSI Type: 6
    Nexthop: 192.168.30.1
    Label  : 24004
    SR-TE Info: N/A
    Source : Remote
    E-Tree : Root
    Layer 2 Attributes:
     DF Role : NDF
     CW   : enabled
     FL   : enabled
     MTU     : 0
     Sig DF  : NDF

Router# show evpn evi inclusive-multicast detail
18         MPLS   0000.0000.0000.0000.0000 0x2   ::  24222
   EtherTag: 2
   Source: Local, MPLS
   Local:
      FRR Label: 0
      Layer 2 Attributes:
       DF Role : Primary
       CW      : Enabled
       FL      : Not Specified
       MTU     : 0
   Num Nexthops: 0
   Path Attributes:
```

show evpn evi ead

To display the EVPN instance (EVI) information, use the **show evpn evi ead** command in the EXEC mode.

show evpn evi ead [**detail** ! **private**]

Syntax Description

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

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.21	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN EVI detailed information:

```
Router#show evpn evi ead detail
Mon Apr 18 13:19:44.311 EDT

EVI   Ethernet Segment Id      EtherTag Nexthop                                Label
----- ----------------------- -------- ---------------------------------------- --------
1     00a1.a2a3.a4a5.a6a7.a8a9 0        ::                                     24006
                                       2.2.2.2                                24007
   Source: Local, Remote, MPLS, VXLAN
1     00a1.a2a3.a4a5.a6a7.a8a9 ffffffff 2.2.2.2                                0
   Source: Remote, Unknown encap
200   0000.0000.0000.0000.0000 1        ::                                     24025
   Source: Local, MPLS
200   0000.0000.0000.0000.0000 4        ::                                     24026
   Source: Local, MPLS
200   0000.0000.0000.0000.0000 11       ::                                     24027
   Source: Local, MPLS
300   00a1.a2a3.a4a5.a6a7.a8a9 0        ::                                     24004
```

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

This sample output shows the EVPN EVI EAD private information:

```
Router#show evpn evi ead private
Mon Apr 18 13:20:31.465 EDT

EVI   Ethernet Segment Id      EtherTag Nexthop                                Label
----- ----------------------- -------- ------------------------------------- --------
1     00a1.a2a3.a4a5.a6a7.a8a9 0        ::                                  24006
                                    2.2.2.2                                 24007
   Source: Local, Remote, MPLS, VXLAN
   EVI: 1
   Num Nexthops: 1

   Object: EVPN EAD
   Base info: version=0xdbdb0013, flags=0x6100, type=24832, reserved=0
   EVPN EAD event history  [Num events: 16]
   ------------------------------------------------------------------------------
     Time                Event                          Flags      Flags
     ====                =====                          =====      =====
     Apr 18 10:55:49.248 Got BGP update                 00000000, 00000001 -  -
     Apr 18 10:55:49.248 Modify_RED                     00000000, 00000000 M  -
     Apr 18 10:55:49.248 Got BGP update                 00000000, 00000001 -  -
     Apr 18 10:55:49.248 Modify_RED                     00000000, 00000000 -  -
     Apr 18 12:03:48.352 Got BGP update                 00000000, 00000001 -  -
     Apr 18 12:04:39.552 Modify_RED                     00000000, 00000000 M  -
     Apr 18 12:04:39.552 Got BGP update                 00000000, 00000001 -  -
     Apr 18 12:04:39.552 Modify_RED                     00000000, 00000000 -  -
     Apr 18 12:15:08.800 Got BGP update                 00000000, 00000001 -  -
     Apr 18 12:15:08.800 Modify_RED                     00000000, 00000000 -  -
     Apr 18 12:15:59.488 Got BGP update                 00000000, 00000001 -  -
     Apr 18 12:19:34.016 Modify_RED                     00000000, 00000000 M  -
     Apr 18 12:19:34.528 Got BGP update                 00000000, 00000001 -  -
     Apr 18 12:19:34.528 Modify_RED                     00000000, 00000000 -  -
     Apr 18 12:19:34.528 Got BGP update                 00000000, 00000001 -  -
     Apr 18 12:19:34.528 Modify_RED                     00000000, 00000000 -  -
   ------------------------------------------------------------------------------

1     00a1.a2a3.a4a5.a6a7.a8a9 ffffffff 2.2.2.2                             0
   Source: Remote, Unknown encap
   EVI: 1
   Num Nexthops: 1

   Object: EVPN EAD
   Base info: version=0xdbdb0013, flags=0x4000, type=16384, reserved=0
   EVPN EAD event history  [Num events: 16]
   ------------------------------------------------------------------------------
     Time                Event                          Flags      Flags
     ====                =====                          =====      =====
     Apr 18 10:55:49.248 Got ESI LABEL                  00000000, 00000000 -  -
     Apr 18 10:55:49.248 Got BGP update                 00000000, 00000001 -  -
     Apr 18 10:55:49.248 Modify_RED                     00000000, 00000000 -  -
     Apr 18 10:55:49.248 Got ESI LABEL                  00000000, 00000000 -  -
     Apr 18 12:03:48.352 Got BGP update                 00000000, 00000001 -  -
     Apr 18 12:03:48.352 Modify_RED                     00000000, 00000000 -  -
     Apr 18 12:03:48.352 Got ESI LABEL                  00000000, 00000000 -  -
     Apr 18 12:04:39.552 Got BGP update                 00000000, 00000001 -  -
```

```
  Apr 18 12:04:39.552 Modify_RED                  00000000, 00000000 -  -
  Apr 18 12:04:39.552 Got ESI LABEL               00000000, 00000000 -  -
  Apr 18 12:15:08.800 Got BGP update              00000000, 00000001 -  -
  Apr 18 12:15:08.800 Modify_RED                  00000000, 00000000 -  -
  Apr 18 12:15:08.800 Got ESI LABEL               00000000, 00000000 -  -
  Apr 18 12:19:34.528 Got BGP update              00000000, 00000001 -  -
  Apr 18 12:19:34.528 Modify_RED                  00000000, 00000000 -  -
  Apr 18 12:19:34.528 Got ESI LABEL               00000000, 00000000 -  -
 ------------------------------------------------------------------------------

200   0000.0000.0000.0000.0000 1        ::                                  24025
 Source: Local, MPLS
 EVI: 200
 Num Nexthops: 0

 Object: EVPN EAD
 Base info: version=0xdbdb0013, flags=0x2100, type=8448, reserved=0
 EVPN EAD event history  [Num events: 4]
 ------------------------------------------------------------------------------
  Time                Event                       Flags      Flags
  ====                =====                       =====      =====
  Apr 18 10:55:45.664 Create                      00000001, 00000000 -  -
  Apr 18 10:55:45.664 Adv to BGP filtered         00002100, 00000000 -  -
  Apr 18 10:55:49.248 EVI REPLAY TO BGP           00000000, 00000000 -  -
  Apr 18 10:55:49.248 Advertise to BGP            00002110, 00000000 -  -
 ------------------------------------------------------------------------------

200   0000.0000.0000.0000.0000 4        ::                                  24026
 Source: Local, MPLS
 EVI: 200
 Num Nexthops: 0

 Object: EVPN EAD
 Base info: version=0xdbdb0013, flags=0x2100, type=8448, reserved=0
 EVPN EAD event history  [Num events: 4]
 ------------------------------------------------------------------------------
  Time                Event                       Flags      Flags
  ====                =====                       =====      =====
  Apr 18 10:55:45.664 Create                      00000001, 00000000 -  -
  Apr 18 10:55:45.664 Adv to BGP filtered         00002100, 00000000 -  -
  Apr 18 10:55:49.248 EVI REPLAY TO BGP           00000000, 00000000 -  -
  Apr 18 10:55:49.248 Advertise to BGP            00002110, 00000000 -  -
 ------------------------------------------------------------------------------

200   0000.0000.0000.0000.0000 11       ::                                  24027
 Source: Local, MPLS
 EVI: 200
 Num Nexthops: 0

 Object: EVPN EAD
 Base info: version=0xdbdb0013, flags=0x2100, type=8448, reserved=0
 EVPN EAD event history  [Num events: 4]
 ------------------------------------------------------------------------------
  Time                Event                       Flags      Flags
  ====                =====                       =====      =====
  Apr 18 10:55:45.664 Create                      00000001, 00000000 -  -
  Apr 18 10:55:45.664 Adv to BGP filtered         00002100, 00000000 -  -
  Apr 18 10:55:49.248 EVI REPLAY TO BGP           00000000, 00000000 -  -
  Apr 18 10:55:49.248 Advertise to BGP            00002110, 00000000 -  -
 ------------------------------------------------------------------------------
```

show evpn internal-label

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

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

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.21	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

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

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

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

show evpn summary

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

show evpn summary[{**location** | **private** | **standby**}]

Syntax Description

location	Displays location specific information.
private	Displays private information.
standby	Displays standby node specific information.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.21	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read

Example

This sample output shows the EVPN summary:

```
Router#show evpn summary
Thu Jul  4 01:34:58.838 DST
-----------------------------
Global Information
-----------------------------
Number of EVIs                : 1
Number of Local MAC Routes    : 1
Number of Remote MAC Routes   : 0
Number of Local IMCAST Routes : 0
Number of Remote IMCAST Routes: 0
Number of Internal Labels     : 0
Number of ES Entries          : 0
BGP Router ID                 : ::
BGP ASN                       : Invalid
PBB BSA MAC address           : f866.f214.abd7
Global peering timer          :     45 seconds
Global recovery timer         :     20 seconds
Global programming timer      :   1500 microseconds
Global flushagain timer       :     60 seconds
-----------------------------
```

```
High Availability Information
-----------------------------
BGP EOD                        : N
Number of Marked MAC Routes    : 0
Number of Swept MAC Routes     : 0
Number of Marked IMCAST Routes: 0
Number of Swept IMCAST Routes : 0
```

staggered-bringup-timer

To stagger the bring-up of bundle interfaces after startup-cost-in timer expiry, use the **staggered-bringup-timer** command in the EVPN configuration mode.

Note The **staggered-bringup-timer** commad is supported in Cisco NCS 5500 Series and Cisco NCS 540 Series Routers.

staggered-bringup-timer *duration*

Syntax Description

duration	Specify the stagger time period. By default, the stagger time is 5000ms and maximum configurable stagger time is 300s.

Command Default

By default, the stagger time is 5000 miliseconds.

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
l2vpn	read, write

This example shows how to configure stagger period:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# staggered-bringup-timer 200s
Router(config-evpn-es)# commit
```

startup-cost-in

To bring up the node into service after the specified time on reload, use the **startup-cost-in** command in EVPN configuration mode. To stop the startup-cost-in timer, use the **no** form of this command.

startup-cost-in *timer*
no startup-cost-in

Syntax Description

startup-cost-in *timer*	Brings up the node into service after the specified time on reload. Specify the time in seconds. Range is from 30 to 86400 seconds.

Command Default

None

Command Modes

EVPN configuration mode

Command History

Release	Modification
Release 6.1.31	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
EVPN	read, write

Examples

The following example shows how to bring up the node into service after the specified time on reload:

```
Router# configure
Router(config)# evpn
Router(config-evpn)# startup-cost-in 6000
Router(config)commit
```

vpws-seamless-integration

To enable EVPN-VPWS seamless integration, use the **vpws-seamless-integration** command in L2VPN configuration mode. To disable EVPN-VPWS seamless integration, use the **no** form of this command.

vpws-seamless-integration

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

L2VPN configuration mode

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
L2VPN	read, write

Examples

The following example shows how to enable EVPN-VPWS integration on an edge device for BGP PW.

```
Router# configure
Router(config)# l2vpn xconnect group 1
Router(config-l2vpn-xc)# mp2mp 2
Router(config-l2vpn-xc-mp2mp)# autodiscovery bgp
Router(config-l2vpn-xc-mp2mp-ad)# signaling-protocol bgp
Router(config-l2vpn-xc-mp2mp-ad-sig)# ce-id 3
Router(config-l2vpn-xc-mp2mp-ad-sig-ce)# vpws-seamless-integration
Router(config-l2vpn-xc-mp2mp-ad-sig-ce)#
```

The following example shows how to enable EVPN-VPWS integration for TLDP PW.

```
Router# configure
Router(config)# l2vpn xconnect group 1
Router(config-l2vpn-xc)# p2p p1
Router(config-l2vpn-xc-p2p)# interface BE1.1
Router(config-l2vpn-xc-p2p)# neighbor 1.1.1.1 pw-id 1
Router(config-l2vpn-xc-p2p)# vpws-seamless-integration
```

weight

To configure the weight of a PE that can be used for EVPN Designated Forwarder (DF) election, use the **weight** command in the EVPN interface Ethernet segment service carving configuration mode.

weight *weight-value*

Syntax Description

weight-value	Specifies the preference DF weight. The range is from 0 to 65535 unless access-driven is configured, in which case it will be 0 to 32767. Default is 32767 when not configured.

Command Default

None

Command Modes

EVPN interface Ethernet segment service carving configuration mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows configuration of DF weight.

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 01.11.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode port-active
Router(config-evpn-ac-es)# service-carving preference-based
Router(config-evpn-ac-es-sc-pref)# weight 100
Router(config-evpn-ac-es-sc-pref)# commit
```

EVPN Routing Policy Language Commands

This section describes the EVPN routing policy language (RPL) commands used to create, modify, monitor, and maintain routing policies.

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 EVPN RPL concepts, configuration tasks, and examples, see the *EVPN Features* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

Note For the rest of the RPL commands, see *Routing Policy Language Commands* chapter in the *Routing Command Reference for Cisco NCS 5500 Series Routers*.

esi in

To match a esi entry in a esi set name or inline esi set, use the **esi in** command in route-policy configuration mode.

esi in {*esi-set-name inline-esi-set parameter*}

Syntax Description

esi-set-name	Name of a esi set. The esi-set accepts H.H.H.H.H value.
inline-esi-set	Inline esi set. The inline esi set must be enclosed in parentheses.
parameter	Parameter name. The parameter name must be preceded with a "$."

Command Default

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 6.1.31	This command was introduced.

Usage Guidelines

Use the **esi in** command as a conditional expression within an **if** statement to match a esi entry in a named esi set or inline esi set.

Note For a list of all conditional expressions available within an **if** statement, see the **if** command.

Task ID

Task ID	Operations
route-policy	read, write

Examples

```
Router(config)# route-policy policy_A
Router(config-rpl)# if esi in (abcd.aaaa.0000.dddd.ffff) then
Router(config-rpl-if)# set local-preference 200
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
```

etag-in

To match a etag entry in a etag set name or inline etag set, use the **etag in** command in route-policy configuration mode.

etag in {*etag-set-name inline-etag-set parameter*}

Syntax Description

etag-set-name	Name of a etag set. The etag-set accepts 32-bit Integer value. Range is 0 to 4294967295.
inline-etag-set	Inline etag set. The inline etag set must be enclosed in parentheses.
parameter	Parameter name. The parameter name must be preceded with a "$."

Command Default

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 6.1.31	This command was introduced.

Usage Guidelines

Use the **etag in** command as a conditional expression within an **if** statement to match a etag entry in a named etag set or inline etag set.

Note For a list of all conditional expressions available within an **if** statement, see the **if** command.

Task ID

Task ID	Operations
route-policy	read, write

Examples

```
Router(config)# route-policy policy_A
Router(config-rpl)# if etag in (200) then
Router(config-rpl-if)# pass
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
```

evpn-gateway

To match the gateway IP address, use the **evpn-gateway in** command in route-policy configuration mode.

evpn-gateway in {*IP addressparameter*}

Syntax Description

IP address	The gateway IP address (32-bit or 128-bit field (IPv4 or IPv6)).
parameter	Parameter name. The parameter name must be preceded with a "$."

Command Default

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 6.1.31	This command was introduced.

Usage Guidelines

Use the **evpn-gateway in** command as a conditional expression within an **if** statement.

Note For a list of all conditional expressions available within an **if** statement, see the **if** command.

Task ID

Task ID	Operations
route-policy	read, write

Examples

```
Router(config)# route-policy policy gateway_A
Router(config-rpl)# if evpn-gateway in (10.0.0.0/24)then
Router(config-rpl-if)# pass
Router(config-rpl-if)# else
Router(config-rpl-else)# drop
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
```

evpn-originator in

To match the originating router's IP address, use the **evpn-originator in** command in route-policy configuration mode.

evpn-originator in {*IP addressparameter*}

Syntax Description

IP address	The originating router's IP address (4 or 16 octets).
parameter	Parameter name. The parameter name must be preceded with a "$."

Command Default

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 6.1.31	This command was introduced.

Usage Guidelines

Use the **evpn-originator in** command as a conditional expression within an **if** statement.

Note For a list of all conditional expressions available within an **if** statement, see the **if** command.

Task ID

Task ID	Operations
route-policy	read, write

Examples

```
Router(config)# route-policy policy originator_A
Router(config-rpl)# if evpn-originator in (10.0.0.0/24) then
Router(config-rpl-if)# set local-preference 100
Router(config-rpl-if)# else
Router(config-rpl-else)# set med 200
Router(config-rpl-else)# endif
Router(config-rpl)# end-policy
```

evpn-route-type is

To match the EVPN route types, use the **evpn-route-type is** command in route-policy configuration mode.

evpn-route-type is {*route types in decimal parameter*}

Syntax Description

route type in decimal	A three bit decimal number. Range is from 1 to 5. • Use route type 1 to specify Ethernet Auto-Discovery Route • Use route type 2 to specify MAC/IP Advertisement Route • Use route type 3 to specify Inclusive Multicast Ethernet Tag Route • Use route type 4 to specify Ethernet Segment Route • Use route type 5 to specify IP Prefix Route
parameter	Parameter name. The parameter name must be preceded with a "$."

Command Default

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 6.1.31	This command was introduced.

Usage Guidelines

Use the **evpn-route-type is** command as a conditional expression within an **if** statement.

Note For a list of all conditional expressions available within an **if** statement, see the **if** command.

Task ID

Task ID	Operations
route-policy	read, write

Examples

```
Router(config)# route-policy policy_A
Router(config-rpl)# if evpn-route-type is 3 then
Router(config-rpl-if)# set local-preference 200
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
```

mac in

To match a mac entry in a mac set name or inline mac set, use the **mac in** command in route-policy configuration mode.

mac in {*mac-set-name inline-mac-set parameter*}

Syntax Description

mac-set-name	Name of a mac-set. The mac-set accepts H.H.H value.
inline-mac-set	Inline mac set. The inline mac set must be enclosed in parentheses.
parameter	Parameter name. The parameter name must be preceded with a "$."

Command Default

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 6.1.31	This command was introduced.

Usage Guidelines

Use the **mac in** command as a conditional expression within an **if** statement to match a mac entry in a named mac set or inline mac set.

Note For a list of all conditional expressions available within an **if** statement, see the **if** command.

Task ID

Task ID	Operations
route-policy	read, write

Examples

```
Router(config)# route-policy policy_A
Router(config-rpl)# if mac in (abcd.1234.ffff) then
Router(config-rpl-if)# set local-preference 300
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
```

Layer 2 Access List Commands

This section describes the commands used to configure Layer 2 access list.

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 Layer 2 Access Control Lists 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*.

ethernet-services access-group

To control access to an interface, use the **ethernet-service access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of the command.

ethernet-services access-group *access-list-name* **ingress**
no ethernet-services access-list *access-list-name* **ingress**

Syntax Description

access-list-name	Name of an Ethernet services access list as specified by the **ethernet-service access-list** command.
ingress	Filters on inbound packets.

Command Default

The interface does not have an Ethernet services access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **ethernet-services access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *access-list-name* argument to specify a particular Ethernet services access list. Use the ingress keyword to filter on inbound packets.

If the list permits the addresses, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns a host unreachable message.

If the specified access list does not exist, all packets are passed.

By default, the unique or per-interface ACL statistics are disabled.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to apply filters on inbound packets from an interface.

```
Router# configure
Router(config)# interface tengige0/0/0/4
Router(config-if)# l2transport
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

ethernet-services access-list

To define an Ethernet services (Layer 2) access list by name, use the **ethernet-services access-list** command in global configuration mode. To remove all entries in an Ethernet services access list, use the **no** form of the command.

ethernet-services access-list *access-list-name*
no ethernet-services access-list *access-list-name*

Syntax Description

access-list-name	Name of the Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.

Command Default

No Ethernet services access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **ethernet-services access-list** command places the router in access list configuration mode, in which the denied or permitted access conditions must be defined.

Only cos (Class of Service) and dei (Discard Eligibility Indication) are supported for Layer 2 ACL.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to configure ethernet-services access-list:

```
Router# configure
Router(config)# ethernet-services access-list es_acl_1
Router(config-es-acl)# 10 deny 00ff.eedd.0010 ff00.0000.00ff 0000.0100.0001 0000.0000.ffff
Router(config-es-acl)# 20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
Router(config-es-acl)# 30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
Router(config-es-acl)# commit
Router(config)# interface tengige0/0/0/4
Router(config-if)# l2transport
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

show access-lists ethernet-services

To display the contents of current Ethernet services access lists, use the **show access-lists ethernet-services** command in EXEC mode.

show access-lists ethernet-services *access-list-name* [**hardware**] **ingress** [**detail**] [**location** {*location* | **all**}]

Syntax Description

access-list-name	Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
hardware	(Optional) Display Ethernet services access list entries in hardware including the match count for a specific ACL in a particular direction across the line card.
ingress	Filters on inbound packets.
detail	(Optional) Display TCAM entries.
location	(Optional) Display information for a specific node number.
location	Fully qualified location specification.
all	Displays packet filtering usage for all interface cards.

Command Default

The contents of all Ethernet services access lists are displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows sample output for the **show access-lists ethernet-services** command:

```
Router# show access-lists ethernet-services es_acl_1 hardware ingress location 0/0/CPU0
Thu Nov  3 22:02:27.222 UTC
ethernet-services access-list es_acl_1
 10 deny any host fcd7.844c.7486 cos 3   (65334 matches)
 20 deny any host fcd7.844c.7486
 30 permit any any

Router# show access-lists ethernet-services es_acl_1 hardware ingress detail location
0/0/CPU0
```

```
Thu Nov  3 22:01:18.620 UTC
es_acl_1 Details:
Sequence Number: 10
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: FCD7:844C:7486
 Destination MAC Mask: FFFF:FFFF:FFFF
COS: 0x03
        Entry Index: 0x0
        DPA Handle: 0x89BF60E8

es_acl_1 Details:
Sequence Number: 20
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: FCD7:844C:7486
 Destination MAC Mask: FFFF:FFFF:FFFF
        Entry Index: 0x0
        DPA Handle: 0x89BF62E8

es_acl_1 Details:
Sequence Number: 30
Number of DPA Entries: 1
ACL ID: 1
ACE Action: PERMIT
ACE Logging: DISABLED
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: 0000:0000:0000
 Destination MAC Mask: 0000:0000:0000
        Entry Index: 0x0
        DPA Handle: 0x89BF64E8

es_acl_1 Details:
Sequence Number: IMPLICIT DENY
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: 0000:0000:0000
 Destination MAC Mask: 0000:0000:0000
        Entry Index: 0x0
        DPA Handle: 0x89BF66E8
```

show access-lists ethernet-services usage pfilter

To identify the modes and interfaces on which a particular access-list is applied, use the **show access-lists ethernet-services usage pfilter** command in EXEC mode. Information displayed includes the application of all or specific access-lists, the interfaces on which they have been applied and the direction in which they are applied.

show access-lists ethernet-services *access-list-name* **usage pfilter location** { *location* | **all** }

Syntax Description

access-list-name	Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
location	Interface card on which the access list information is needed.
location	Fully qualified location specification.
all	Displays packet filtering usage for all interface cards.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to display packet filter usage at a specific location:

```
Router# show access-lists ethernet-services es_acl_1 usage pfilter location 0/0/CPU0
Thu Nov  3 21:58:19.706 UTC
Interface : TenGigE0/0/0/0/1
    Input ACL : es_acl_1
    Output ACL : N/A
```

Multiple Spanning Tree Protocol Commands

This module describes the commands used to configure multiple spanning tree protocol. For detailed information about MSTP concepts, configuration tasks, and examples, see the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

instance (MSTP)

In order to configure the multiple spanning tree instance (MSTI), use the **instance** command in MSTP configuration submode.

instance *id*

Syntax Description

id	MSTI ID. Range is 0 to 4094.

Command Default

None

Command Modes

MSTP configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

Note An instance ID of 0 represents the Common Internal Spanning Tree (CIST) for the region.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MSTI configuration submode:

```
RP/0/RP0/CPU0:router(config-mstp)# instance 101
RP/0/RP0/CPU0:router(config-mstp-inst)#
```

interface (MSTP)

To enter the MSTP interface configuration submode, use the **interface** command in MSTP configuration submode.

interface *interface-type interface-path-id*

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical 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

MSTP configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

A given port may only be enabled with MSTP or PVRST.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MSTP interface configuration submode:

```
Router(config-mstp)# interface GigabitEthernet 0/0/0/7
```

name (MSTP)

To set the name of the MSTP region, use the **name** command in MSTP configuration submode.

name *name*

Syntax Description

name	String of a maximum of 32 characters conforming to the definition of SnmpAdminString in RFC 2271.

Command Default

The MAC address of the switch, formatted as a text string using the hexadecimal representation specified in IEEE Std 802.

Command Modes

MSTP configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to set the name of the MSTP region to m1:

```
RP/0/RP0/CPU0:router(config-mstp)# name m1
```

portfast

To enable PortFast feature on the port and enable BPDU guard, use the **portfast** command in MSTP interface configuration submode.

portfast [**bpduguard**]

Syntax Description

This command has no keywords or arguments.

Command Default

PortFast is disabled.

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

This command enables the portfast feature (also known as edge port). When this is enabled, MSTP treats the port as an edge port, i.e., it keeps it in forwarding state and does not generate topology changes if the port goes down or comes up. It is not expected to receive MSTP BPDUs on an edge port. BPDU guard is a Cisco extension that causes the interface to be shut down using error-disable if an MSTP BPDU is received.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enable PortFast and BPDU guard on the port:

```
Router(config-mstp-if)# portfast
Router(config-mstp-if)# portfast bpduguard
```

show spanning-tree mst

To display the multiple spanning tree protocol status information, use the **show spanning-tree mst** command in EXEC mode.

show spanning-tree mst *protocol-instance-identifier* [**instance** *instance-id*] [{**blocked-ports** | **brief**}]

Syntax Description

protocol-instance-identifier	String of a maximum of 25 characters that identifies the protocol instance.
instance *instance-id*	Forward interface in rack/slot/instance/port format.
brief	Displays a summary of MST information only.
blocked-ports	Displays MST information for blocked ports only.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows the output from the **show spanning-tree mst** command, which produces an overview of the spanning tree protocol state:

```
RP/0/RP0/CPU0:router# show spanning-tree mst a instance 0
Operating in Provider Bridge mode
MSTI 0 (CIST):

  VLANS Mapped: 1-100, 500-1000, 1017

  Root ID    Priority    4097
             Address     0004.9b78.0800
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec


  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     0004.9b78.0800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Interface                Port ID                     Designated               Port ID
Name                     Prio.Nbr Cost   Role State  Cost Bridge ID           Prio.Nbr
-----------------------  -------- ------ ---------  ------------------------ --------
GigabitEthernet0/1/2/1   128.65   20000  DSGN FWD    0    4097 0004.9b78.0800 128.65
GigabitEthernet0/1/2/2   128.66   20000  DSGN FWD    0    4097 0004.9b78.0800 128.66
...
```

The following example shows the output from the **show spanning-tree mst** command when the **brief** and **blocked-ports** keywords are used:

```
RP/0/RP0/CPU0:router# show spanning-tree mst a brief
MSTI 0 (CIST):
  VLAN IDs: 1-100, 500-1000, 1017
  This is the Root Bridge
MSTI 1:
  VLAN IDS: 101-499
  Root Port GigabitEthernet0/1/2/2  , Root Bridge ID 0002.9b78.0812
...
RP/0/RP0/CPU0:router# show spanning-tree mst blocked-ports
MSTI 0 (CIST):

Interface                Port ID                     Designated               Port ID
Name                     Prio.Nbr Cost   Role State  Cost Bridge ID           Prio.Nbr
-----------------------  -------- ------ ---------  ------------------------ --------
GigabitEthernet0/0/4/4      128.196  200000 ALT  BLK    0    4097 0004.9b78.0800 128.195
...
```

spanning-tree mst

To enter the MSTP configuration submode, use the **spanning-tree mst** command in global configuration mode.

spanning-tree mst *protocol-instance-identifier*

Syntax Description

protocol-instance-identifier	String of a maximum of 25 characters that identifies the protocol instance.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

Note In MSTP configuration, only one protocol instance can be configured at a time.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MSTP configuration submode:

```
Router(config)# spanning-tree mst m0
```

vlan-ids (MSTP)

To associate a set of VLAN IDs with the current MSTI, use the **vlan-ids** command in MSTI configuration submode.

vlan-ids *vlan-range-list*

Syntax Description

vlan-range-list	A comma-separated list of VLAN ranges in the form a-b, c, d, e-f, g etc. Upto 3 ranges can be specified.

Command Default

None

Command Modes

MSTI configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to use the vlan-id command:

```
RP/0/RP0/CPU0:router(config-mstp-inst)# vlan-ids 2-1005
```

MSTP BPDU Guard Commands

This section describes the commands used to configure MSTP BPDU Guard.

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
  - 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 MSTP BPDU Guard 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 (MSTP), on page 211
- portfast, on page 212
- spanning-tree mst, on page 213

interface (MSTP)

To enter the MSTP interface configuration submode, use the **interface** command in MSTP configuration submode.

interface *interface-type interface-path-id*

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical 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

MSTP configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

A given port may only be enabled with MSTP or PVRST.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MSTP interface configuration submode:

```
Router(config-mstp)# interface GigabitEthernet 0/0/0/7
```

portfast

To enable PortFast feature on the port and enable BPDU guard, use the **portfast** command in MSTP interface configuration submode.

portfast [**bpduguard**]

Syntax Description

This command has no keywords or arguments.

Command Default

PortFast is disabled.

Command Modes

MSTP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

This command enables the portfast feature (also known as edge port). When this is enabled, MSTP treats the port as an edge port, i.e., it keeps it in forwarding state and does not generate topology changes if the port goes down or comes up. It is not expected to receive MSTP BPDUs on an edge port. BPDU guard is a Cisco extension that causes the interface to be shut down using error-disable if an MSTP BPDU is received.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enable PortFast and BPDU guard on the port:

```
Router(config-mstp-if)# portfast
Router(config-mstp-if)# portfast bpduguard
```

spanning-tree mst

To enter the MSTP configuration submode, use the **spanning-tree mst** command in global configuration mode.

spanning-tree mst *protocol-instance-identifier*

Syntax Description

protocol-instance-identifier	String of a maximum of 25 characters that identifies the protocol instance.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

Note In MSTP configuration, only one protocol instance can be configured at a time.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to enter the MSTP configuration submode:

```
Router(config)# spanning-tree mst m0
```

VXLAN Commands

This section describes the commands used to configure VXLAN.

host-reachability protocol static

To configure the static control protocol for VXLAN tunnel endpoint reachability, use the **host-reachability protocol static** command in NVE interface configuration mode.

host-reachability protocol static

Command Default

None

Command Modes

NVE interface configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	read, write
tunnel	read, write

Example

The following example shows control protocol configuration for VXLAN tunnel endpoint reachability.

```
Router(config)# interface nve1
Router(config-if)# member vni 2
Router(config-nve-vni)# host-reachability protocol static
Router(config-nve-vni)# commit
```

interface nve

To create a network virtualization endpoint (NVE) interface and enter the NVE interface configuration mode, use the **interface nve** command in global configuration mode. To remove the NVE interface, use the **no** form of this command.

interface nve *nve-id*

Syntax Description

nve-id	The NVE interface ID. It can take values from 1 to 65535.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	read, write

Example

The following example shows how to create an NVE interface and enter the NVE interface configuration mode.

```
Router(config)# interface nve 1
Router(config-if)#
```

member vni

To map VXLAN to a network virtualization endpoint (NVE) interface, use the **member vni** command in the NVE interface configuration mode. To remove the VXLAN from the interface, use the **no** form of this command.

member vni *vni-number*

Syntax Description

vni-number	The ID of the VXLAN to be mapped to the NVE. The valid values are from 1 to 16777215.

Command Default

None

Command Modes

NVE interface configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	read, write
tunnel	read, write

Example

The following example shows the VXLAN with VNI "2" associated with the NVE "1".

```
Router(config)# interface nve 1
Router(config-if)# member vni 2
```

overlay-encapsulation vxlan

To define VXLAN as the encapsulation type for Network Virtualization Endpoint (NVE) interface, use the **overlay-encapsulation vxlan** command in NVE interface configuration mode. To remove the configured encapsulation on the NVE interface, use the **no** form of this command.

overlay-encapsulation vxlan

Command Default

None

Command Modes

NVE interface configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	read, write
tunnel	read, write

Example

The following example shows an NVE interface configured for VXLAN encapsulation.

```
Router# configure
Router(config)# interface nve1
Router(config-if)# overlay-encapsulation vxlan
Router(config-nve-encap-vxlan)# commit
```

show nve interface

To display the network virtualization endpoint (NVE) interface information, use the **show nve interface** command in XR EXEC mode.

show nve interface [{ **detail** | **nve** *nve-id* }]

Syntax Description

detail	Displays detailed information about NVE interfaces.
nve *nve-id*	Displays information only about the specified NVE interface.

Command Default

None

Command Modes

XR EXEC

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	read

Example

This is the sample output of the **show interface nve** command anycast gateway parameters.

```
Router# show interface nve100 detail
Interface: nve100 State: Up Encapsulation: VxLAN
  Source Interface: Loopback1 (primary: 10.0.0.1)
  Source Interface State: Up
  NVE Flags: 0x1, Admin State: Up, Interface Handle 0xba0
  UDP Port: 4789
  Anycast Source Interface: Loopback100 (primary: 100.1.1.1)
```

show nve vni

To display list of all VNIs that are associated with various NVE interfaces and the associated multicast IP address that is used for multi-destination frames, use the **show nve vni** command in XR EXEC mode.

show nve vni [{ **vni_number** | **detail** | **interface nve** *nve-id* }]

Syntax Description

vni_number	Displays output for the specific VNI.
detail	Displays more detailed output.
interface nve *nve-id*	Displays details for the specific NVE interface.

Command Default

None

Command Modes

XR EXEC

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
tunnel	read

Example

The following shows an example output of this show command:

```
Router# show nve vni
Interface  VNI          MCAST        VNI State        Mode
nve3       1002         0.0.0.0      Up               L3 Control (Static)
nve1       17001        0.0.0.0      Up               L3 Control (Static)
nve2       17002        0.0.0.0      Up               L3 Control (Static)
nve3       17003        0.0.0.0      Up               L3 Control (Static)
```

source-interface loopback

To specify a loopback interface whose IP address should be set as the IP address for the NVE interface, use the **source-interface loopback** command.

source-interface loopback *interface-id*

Syntax Description

loopback	Specifies a loopback interface as providing IP address for the NVE interface.
interface-id	Specifies the loopback interface ID. It can take values from 0 to 65535.

Command Default

None

Command Modes

NVE interface configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
tunnel	read, write
interface	read, write

Example

The following example shows how to configure the IP address of an NVE interface as the IP address of a loopback interface.

```
Router(config)# interface nve 1
Router(config-if)# source-interface loopback 1
```