



## **Interface and Hardware Component Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.5.x**

**First Published:** 2021-11-01

**Last Modified:** 2023-09-29

### **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 NON-INFRINGEMENT 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](http://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)

© 2021 Cisco Systems, Inc. All rights reserved.



# CONTENTS

---

## PREFACE

### **Preface** xiii

Changes to This Document xiii

Communications, Services, and Additional Information xiii

---

## CHAPTER 1

### **New and Changed Feature Information** 1

Interface and Hardware Component Features Added or Modified in IOS XR Release 7.5.x 1

---

## CHAPTER 2

### **Preconfiguring Physical Interfaces** 3

Prerequisites for Preconfiguring Physical Interfaces 3

Information About Preconfiguring Physical Interfaces 4

Physical Interface Preconfiguration Overview 4

Benefits of Interface Preconfiguration 4

Use of the Interface Preconfigure Command 4

Active and Standby RPs and Virtual Interface Configuration 5

How to Preconfigure Physical Interfaces 5

---

## CHAPTER 3

### **Advanced Configuration and Modification of the Management Ethernet Interface** 7

Prerequisites for Configuring Management Ethernet Interfaces 7

Information About Configuring Management Ethernet Interfaces 8

Default Interface Settings 8

How to Perform Advanced Management Ethernet Interface Configuration 8

Configure a Management Ethernet Interface 8

Verify Management Ethernet Interface Configuration 11

Configuration Examples for Management Ethernet Interfaces 11

Configuring a Management Ethernet Interface: Example 11

---

<b>CHAPTER 4</b>	<b>Configuring Ethernet Interfaces</b>	<b>13</b>
	Prerequisites for Configuring Ethernet Interfaces	14
	Information About Configuring Ethernet	14
	Cisco 8000 Modular Line Cards	14
	Default Configuration Values for 100-Gigabit Ethernet	14
	Layer 2 VPN on Ethernet Interfaces	15
	Gigabit Ethernet Protocol Standards Overview	15
	IEEE 802.3 Physical Ethernet Infrastructure	16
	IEEE 802.3ae 10-Gbps Ethernet	16
	IEEE 802.3ba 100 Gbps Ethernet	16
	MAC Address	16
	Ethernet MTU	16
	IP MTU	17
	IP MTU Checks	18
	IP MTU Configuration Guidelines	19
	IP MTU Limitations and Feature Support	21
	IP MTU Scale	22
	Configure IP MTU	22
	Flow Control on Ethernet Interfaces	24
	802.1Q VLAN	25
	Subinterfaces on the Router	25
	Layer 2, Layer 3, and EFPs	28
	Enhanced Performance Monitoring for Layer 2 Subinterfaces (EFPs)	30
	Other Performance Management Enhancements	31
	Frequency Synchronization and SyncE	31
	LLDP	31
	LLDP Frame Format	32
	LLDP TLV Format	32
	Specifying User-Defined LLDP TLV Values	33
	LLDP Operation	34
	Supported LLDP Functions	35
	Unsupported LLDP Functions	35
	Setting the Carrier Delay on Physical Interfaces	36

How to Configure Ethernet	37
Configuring LLDP	37
LLDP Default Configuration	38
Enabling LLDP Per Interface	38
Enabling LLDP Globally	39
Configuring Global LLDP Operational Characteristics	40
Disabling Transmission of Optional LLDP TLVs	41
Disabling LLDP Receive and Transmit Operation for an Interface	43
Verifying the LLDP Configuration	44
Verifying the LLDP Global Configuration	44
Verifying the LLDP Interface Configuration	45
Configuration Examples for Ethernet	46
Configuring an Ethernet Interface: Example	46
Configuring LLDP: Examples	46
Configuring a Layer 2 VPN AC: Example	47
Configuring Physical Ethernet Interfaces	47
Viewing Interface Counters Report	51
Instant Display of Traffic Rates for all the Physical Interfaces	52
How to Configure Interfaces in Breakout Mode	53
Information About Breakout	53
Configure Breakout in a Port	53
Remove the Breakout Configuration	53
Verify a Breakout Configuration	54

---

**CHAPTER 5**

<b>Configuring Ethernet OAM</b>	<b>55</b>
Information About Configuring Ethernet OAM	55
Ethernet Link OAM	56
Neighbor Discovery	56
EFD	57
MIB Retrieval	57
Miswiring Detection (Cisco-Proprietary)	58
SNMP Traps	58
Configuring Ethernet OAM	58
Configuring an Ethernet OAM Profile	58

Attaching an Ethernet OAM Profile to an Interface	63
Configuring Ethernet OAM at an Interface and Overriding the Profile Configuration	64
Verifying the Ethernet OAM Configuration	66
Configuration Examples for Ethernet OAM	66
Configuring Ethernet OAM Features on an Individual Interface: Example	66
Configuring an Ethernet OAM Profile Globally: Example	67
Configuring Ethernet OAM Features to Override the Profile on an Individual Interface: Example	67
Clearing Ethernet OAM Statistics on an Interface: Example	68
Enabling SNMP Server Traps on a Router: Example	68
Ethernet CFM	69
Maintenance Domains	70
Services	73
Maintenance Points	73
MEP and CFM Processing Overview	73
CFM Protocol Messages	75
Continuity Check (IEEE 802.1ag and ITU-T Y.1731)	75
Loopback (IEEE 802.1ag and ITU-T Y.1731)	78
Linktrace (IEEE 802.1ag and ITU-T Y.1731)	79
Configurable Logging	81
How to Configure Ethernet OAM	81
Configuring Ethernet OAM	81
Configuring an Ethernet OAM Profile	81
Attaching an Ethernet OAM Profile to an Interface	87
Configuring Ethernet OAM at an Interface and Overriding the Profile Configuration	88
Verifying the Ethernet OAM Configuration	89
Configuring Ethernet CFM	90
Configuring a CFM Maintenance Domain	90
Configuring Services for a CFM Maintenance Domain	91
Enabling and Configuring Continuity Check for a CFM Service	93
Configuring Cross-Check on a MEP for a CFM Service	94
Configuring Other Options for a CFM Service	96
Configuring CFM MEPs	98
Configuring Y.1731 AIS	100
Verifying the CFM Configuration	103

CFM Over Bundles	103
Ethernet Frame Delay Measurement for L2VPN Services	104

**CHAPTER 6**

<b>IP Event Dampening</b>	<b>109</b>
IP Event Dampening Overview	109
Interface State Change Events	110
Suppress Threshold	110
Half-Life Period	110
Reuse Threshold	110
Maximum Suppress Time	111
Affected Components	111
Route Types	111
Supported Protocols	111
How to Configure IP Event Dampening	112
Enabling IP Event Dampening	112
Verifying IP Event Dampening	112

**CHAPTER 7**

<b>Configuring Link Bundling</b>	<b>113</b>
Limitations and Compatible Characteristics of Ethernet Link Bundles	114
Prerequisites for Configuring Link Bundling on a Router	115
Information About Configuring Link Bundling	116
Link Bundling Overview	116
Link Aggregation Through LACP	116
IEEE 802.3ad Standard	117
Configuring LACP Fallback	117
LACP Short Period Time Intervals	118
Load Balancing	119
Layer 3 Egress Load Balancing on Link Bundles	119
Configuring the Default LACP Short Period Time Interval	120
Configuring Custom LACP Short Period Time Intervals	122
QoS and Link Bundling	126
Link Bundle Configuration Overview	126
Nonstop Forwarding During Card Failover	127
Link Failover	127

Link Switchover	127
LACP Fallback	128
How to Configure Link Bundling	128
Configuring Ethernet Link Bundles	128
Configuring VLAN Bundles	132
132	
VLANs on an Ethernet Link Bundle	135
Configuration Examples for Link Bundling	136
Example: Configuring an Ethernet Link Bundle	136
Example: Configuring a VLAN Link Bundle	138

**CHAPTER 8****Configuring Traffic Mirroring 139**

Introduction to Traffic Mirroring	140
Implementing Traffic Mirroring on the Cisco 8000 Series Routers	141
ERSPAN	141
Traffic Mirroring Terminology	144
Characteristics of the Source Port	144
Characteristics of the Monitor Session	145
Supported Traffic Mirroring Types	145
ACL-Based Traffic Mirroring	146
ERSPAN over GRE IPv6	146
Configuring Partial Packet Capture Ability for ERSPAN (RX)	148
ERSPAN Traffic to a Destination in a Non-Default VRF	149
Restrictions for Traffic Mirroring	149
Configuring Traffic Mirroring	150
Configuring ACLs for Traffic Mirroring	150
Troubleshooting ACL-Based Traffic Mirroring	152
Flexible CLI for ERSPAN	153
Attaching the Configurable Source Interface	154
Introduction to ERSPAN Rate Limit	155
Topology	156
Configure ERSPAN Rate Limit	156
Introduction to File Mirroring	157
Limitations	158



Configure File Mirroring	158
Introduction to Local SPAN	159
Local SPAN Overview	159
Local SPAN Supported Capabilities	159
Local SPAN Restrictions	160
Configuring Local SPAN	160
Local SPAN with ACL	161
Configuring Local SPAN with ACL	161
Local SPAN Rate Limit	162
Traffic Mirroring with DSCP	163
DSCP Marking on Egress GRE Tunnel in ERSPAN	164
Configure DSCP Marking on Egress GRE Tunnel in ERSPAN	164
DSCP Bitmask to Filter Ingress ERSPAN Traffic	166
Configure DSCP Bitmask to Filter Ingress ERSPAN Traffic	166
Monitor Multiple ERSPAN Sessions with SPAN and Security ACL	168
Configure Multiple Monitor ERSPAN Sessions with SPAN and Security ACL	168
SPAN to File	169
Action Commands for SPAN to File	171
Configuring SPAN to File	172
Configuring SPAN to File for Truncation and Direction	174
Mirroring Forward-Drop Packets	175
Configuring Forward-Drop	176
Traffic Mirroring Configuration Examples	177
Viewing Monitor Session Status: Example	177
Monitor Session Statistics: Example	178
Layer 3 ACL-Based Traffic Mirroring: Example	179
Troubleshooting Traffic Mirroring	179

---

**CHAPTER 9**

<b>Configuring Virtual Loopback and Null Interfaces</b>	<b>185</b>
Prerequisites for Configuring Virtual Interfaces	185
Information About Configuring Virtual Interfaces	185
Virtual Loopback Interface Overview	186
Null Interface Overview	186
Virtual Management Interface Overview	186

Active and Standby RPs and Virtual Interface Configuration	187
How to Configure Virtual Interfaces	187
Configuring Virtual Loopback Interfaces	187
Configuring Null Interfaces	188
Configuring Virtual IPv4 Interfaces	188
Configuration Examples for Virtual Interfaces	189
Configuring a Loopback Interface: Example	189
Configuring a Null Interface: Example	190
Configuring a Virtual IPv4 Interface: Example	190

**CHAPTER 10****Configure GRE Tunnels 191**

GRE Tunnels	191
Supported Features on a GRE Tunnel	193
Limitations for Configuring GRE Tunnels	194
Configure GRE Tunnels	195
Unidirectional GRE Encapsulation (GREv4)	196
Unidirectional GRE Decapsulation (GREv4)	196
ECMP and LAG Hashing for NVGRE Flows	198

**CHAPTER 11****Configuring 802.1Q VLAN Interfaces 201**

Prerequisites for Configuring 802.1Q VLAN Interfaces	201
Information About Configuring 802.1Q VLAN Interfaces	202
802.1Q VLAN Overview	202
Subinterfaces	202
Subinterface MTU	202
Native VLAN	203
Layer 2 VPN on VLANs	203
How to Configure 802.1Q VLAN Interfaces	203
Configuring 802.1Q VLAN Subinterfaces	203
Configuring an Attachment Circuit on a VLAN	205
Removing an 802.1Q VLAN Subinterface	207
Configuration Examples for VLAN Interfaces	208
VLAN Subinterfaces: Example	208

---

<b>CHAPTER 12</b>	<b>Configure IP-in-IP Tunnels</b>	<b>211</b>
	IP-in-IP Decapsulation	214
	Decapsulation Using Tunnel Source Direct	217
	Configure Tunnel Destination with an Object Group	219
	ECMP Hashing Support for Load Balancing	222
	User-Defined Fields for ECMP Hashing	224
	Configure User-Defined Fields for ECMP Hashing	225

---

<b>CHAPTER 13</b>	<b>Configuring Generic UDP Encapsulation</b>	<b>229</b>
	Understand Generic UDP Encapsulation	229
	Restrictions	231
	Configure GUE	231

---

<b>CHAPTER 14</b>	<b>Controlling the TTL Value of Inner Payload Header</b>	<b>235</b>
	IP-in-IP Decapsulation	236
	Decapsulation Using Tunnel Source Direct	239
	Configure Tunnel Destination with an Object Group	241
	ECMP Hashing Support for Load Balancing	244
	User-Defined Fields for ECMP Hashing	246
	Configure User-Defined Fields for ECMP Hashing	247

---

<b>CHAPTER 15</b>	<b>Configuring 400G Digital Coherent Optics</b>	<b>251</b>
	Configuring Frequency	255
	Configuring Chromatic Dispersion	257
	Configuring Optical Transmit Power	259
	Configuring Muxponder Mode	261
	Configuring Modulation	262
	Configuring DAC Rate	264
	Configuring FEC	266
	Configuring Loopback	267
	Configuring Performance Monitoring	268
	Configuring PM Parameters	268
	Configuring Alarms Threshold	272

---

**CHAPTER 16****Configuring Controllers 275**

- How to Configure Controllers 276
  - Configuring Optics Controller 276
  - Disabling Optical Modules 276
- Diagnostic Parameters for Optical Transceivers 279
- Loopback on Optical Transceivers 285
- Media Side Input Loopback Configuration 287
- Media Side Output Loopback 288
- Host Side Input Loopback Configuration 289
- Host Side Output Loopback Configuration 291



## Preface

This guide describes the Netflow configuration details for Cisco IOS XR software. This chapter contains details on the changes made to this document.

- [Changes to This Document, on page xiii](#)
- [Communications, Services, and Additional Information, on page xiii](#)

## 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
March 2023	Republished with feature updates for Release 7.5.4.
September 2022	Republished with feature updates for Release 7.5.3.
April 2022	Republished with feature updates for Release 7.5.2.
November 2021	Initial release of this document.

## Communications, Services, and Additional Information

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

### **Cisco Bug Search Tool**

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



## CHAPTER

# 1

## New and Changed Feature Information

This table summarizes the new and changed feature information for the *Interfaces Configuration Guide for Cisco 8000 Series Routers* for Cisco 8000 Series Routers, and tells you where they are documented.

- [Interface and Hardware Component Features Added or Modified in IOS XR Release 7.5.x](#), on page 1

## Interface and Hardware Component Features Added or Modified in IOS XR Release 7.5.x

This table summarizes the new and changed feature information for the *Interfaces Configuration Guide for Cisco 8000 Series Routers* for Cisco 8000 Series Routers, and tells you where they are documented.

**Table 2: New and Changed Features**

Feature	Description	Introduced in Release	Where Documented
User-Defined Fields for ECMP Hashing	This feature was introduced.	Release 7.5.5	<a href="#">User-Defined Fields for ECMP Hashing</a>
Diagnostic Parameters for Optical Transceivers	This feature was introduced.	Release 7.5.5	<a href="#">Diagnostic Parameters for Optical Transceivers</a> , on page 279
Loopback on Optical Transceivers	This feature was introduced.	Release 7.5.5	<a href="#">Loopback on Optical Transceivers</a> , on page 285
Traffic Mirroring with DSCP	This feature was introduced.	Release 7.5.4	<a href="#">Traffic Mirroring with DSCP</a>
Instant Display of Traffic Rates for all the Physical Interfaces	This feature was introduced.	Release 7.5.4	<a href="#">Viewing Interface Counters Report</a>
Configure Tunnel Destination with an Object Group	This feature was introduced.	Release 7.5.4	<a href="#">Configure Tunnel Destination with an Object Group</a> , on page 219

Feature	Description	Introduced in Release	Where Documented
Specifying User-Defined LLDP TLV Values	This feature was introduced.	Release 7.5.3	<a href="#">Specifying User-Defined LLDP TLV Values, on page 33</a>
Partial Packet Capture Ability for ERSPAN (RX)	This feature was introduced.	Release 7.5.3	<a href="#">ERSPAN</a>
SPAN to File Support for TX and RX	This feature was introduced.	Release 7.5.3	<a href="#">SPAN to File</a>
Partial Packet Capture Ability for SPAN to File (RX)	This feature was introduced.	Release 7.5.3	<a href="#">SPAN to File</a>
Ethernet Frame Delay Measurement for L2VPN Services	This feature was introduced.	Release 7.5.3	<a href="#">Ethernet Frame Delay Measurement for L2VPN Services, on page 104</a>
ERSPAN Traffic to a Destination in a Non-Default VRF	This feature was introduced.	Release 7.5.2	<a href="#">ERSPAN Traffic to a Destination in a Non-Default VRF, on page 149</a>
IP MTU	This feature was introduced.	Release 7.5.2	<a href="#">IP MTU, on page 17</a>





## CHAPTER 2

# Preconfiguring Physical Interfaces

This module describes the preconfiguration of physical interfaces.

The system supports preconfiguration for the following interfaces:

- 10-Gigabit Ethernet
- 40-Gigabit Ethernet
- 100-Gigabit Ethernet
- 400-Gigabit Ethernet
- Management Ethernet

Preconfiguration allows you to configure line cards before you insert them into the router. When you insert the cards, they are instantly configured. The system creates the preconfiguration information in a different system database tree, rather than with the regularly configured interfaces. That database tree is known as the *preconfiguration directory* on the Route Processor.

There might be some preconfiguration data that you cannot verify unless the line card is present. This is because the verifiers themselves run only on the line card. You can verify such preconfiguration data when you insert the line card and initiate the verifiers. The system rejects a configuration if errors are found when you copy the configuration from the preconfiguration area to the active area.



---

**Note** Gigabit Ethernet interface is not supported. You can only preconfigure physical interfaces.

---

- [Prerequisites for Preconfiguring Physical Interfaces, on page 3](#)
- [Information About Preconfiguring Physical Interfaces, on page 4](#)
- [How to Preconfigure Physical Interfaces, on page 5](#)

## Prerequisites for Preconfiguring Physical Interfaces

Before preconfiguring physical interfaces, ensure that you meet the following condition(s):

- Preconfiguration drivers and files are installed. Although it might be possible to preconfigure physical interfaces without a preconfiguration driver installed. The preconfiguration files are required to set the interface definition file on the router that supplies the strings for valid interface names.

# Information About Preconfiguring Physical Interfaces

To preconfigure interfaces, you must understand the following concepts:

## Physical Interface Preconfiguration Overview

Preconfiguration is the process of configuring interfaces before they are present in the system. You cannot verify or apply preconfigured interfaces until you insert the actual interface into the router with the matching location. The location can be the rack, slot, or module. When you insert the anticipated line card and create the interface, the system verifies the precreated configuration information. If the verification is successful, the system immediately applies the running configuration of the router.



---

**Note** When you plug the anticipated line card in, ensure that you verify any preconfiguration by using the appropriate **show** commands.

---

Use the **show run** command to see the interfaces that are in the preconfigured state.



---

**Note** We recommend filling out preconfiguration information in your site planning guide. This allows you to compare the anticipated configuration with the actual preconfigured interfaces when you install the card and the interfaces are up.

---



---

**Tip** Use the **commit best-effort** command to save the preconfiguration to the running configuration file. The **commit best-effort** command merges the target configuration with the running configuration and commits only the valid configuration (best effort). Some configuration might fail due to semantic errors, but the valid configuration still comes up.

---

## Benefits of Interface Preconfiguration

Preconfigurations reduce downtime when you add new cards to the system. With preconfiguration, you can instantly configure the new modular services card that actively runs during the line card bootup.

Another advantage of performing a preconfiguration is that during a card replacement, when you remove the line card, you can still see the previous configuration and make modifications.

## Use of the Interface Preconfigure Command

To preconfigure the interfaces that are not yet present in the system, use the **interface preconfigure** command in global configuration mode.

The **interface preconfigure** command places the router in interface configuration mode. You must be able to add any possible interface commands. The verifiers registered for the preconfigured interfaces verify the

configuration. The preconfiguration is complete when you enter the **end** command, or any matching exit or global configuration mode command.



---

**Note** It is possible that you are not able to verify some configurations until you insert the line card is inserted. Do not enter the **no shutdown** command for new preconfigured interfaces, because the no form of this command removes the existing configuration, and there is no existing configuration.

---

You must provide names during preconfiguration that matches with the name of the interface that is created. If the interface names do not match, the system does not apply preconfiguration when the interface is created. The interface names must begin with the interface type that is supported by the router and for which drivers have been installed. However, the slot, port, subinterface number, and channel interface number information cannot be validated.



---

**Note** Specifying an interface name that already exists and is configured (or an abbreviated name like Hu0/3/0/0) is not permitted.

---

## Active and Standby RPs and Virtual Interface Configuration

The standby RP is available and is in a state in which it can take the load from the an active RP, if required. Following are the conditions when a standby RP becomes an active RP:

- Failure detection by a watchdog.
- Standby RP is administratively commanded to take over.
- Removal of the active RP from the chassis.

If a second RP is not present in the chassis while the first is in operation, the system may insert a second RP. The second RP then automatically becomes the standby RP. The standby RP may also be removed from the chassis with no effect on the system other than loss of RP redundancy.

After failover, the virtual interfaces become available on the standby (now active) RP. Their state and configuration is unchanged, and there is no loss of forwarding (in the case of tunnels) over the interfaces during the failover. The routers use nonstop forwarding (NSF) over tunnels through the failover of the host RP.



---

**Note** You do not need to configure anything to guarantee that the standby interface configurations are maintained.

---

## How to Preconfigure Physical Interfaces

This task describes only the most basic preconfiguration of an interface.

```
/* Enter global configuration mode. */  
RP/0/RP0/CPU0:router:router:hostname# configure
```

```
/* Enters interface preconfiguration mode for an interface, where type specifies
the supported interface type that you want to configure and interface-path-id specifies
the location where the interface will be located in rack/slot/module/port notation. */
```

```
RP/0/RP0/CPU0:router:router(config)# interface preconfigure HundredGigE 0/3/0/2
```

```
/* Assign an IP address and mask to the interface. Use one of the following commands:
```

```
- ipv4 address ip-address subnet-mask
```

```
- ipv4 address ip-address/prefix */
```

```
RP/0/RP0/CPU0:router(config-if-pre)# ipv4 address 192.168.1.2/31
```

```
RP/0/RP0/CPU0:router(config-if-pre)# end
```

```
or
```

```
RP/0/RP0/CPU0:router(config-if-pre)# commit
```

```
RP/0/RP0/CPU0:router# show running-config
```

- When you issue the **end** command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)?
- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit best-effort** command to save the configuration changes to the running configuration file and remain within the configuration session. The **commit best-effort** command merges the target configuration with the running configuration and commits only valid changes (best effort). Some configuration changes might fail due to semantic errors.



## CHAPTER 3

# Advanced Configuration and Modification of the Management Ethernet Interface

---

This module describes the configuration of Management Ethernet interfaces.

Before you use Telnet to access the router through the LAN IP address, you must set up a Management Ethernet interface and enable the Telnet servers.



---

**Note** By default, the Management Ethernet interfaces are present on the system. However, you must configure these interfaces to:

- Access the router.
- Use protocols and applications, such as Simple Network Management Protocol (SNMP), HTTP, eXtensible Markup Language (XML), TFTP, Telnet, and Command-Line Interface (CLI.)

- 
- [Prerequisites for Configuring Management Ethernet Interfaces, on page 7](#)
  - [Information About Configuring Management Ethernet Interfaces, on page 8](#)
  - [How to Perform Advanced Management Ethernet Interface Configuration, on page 8](#)
  - [Configuration Examples for Management Ethernet Interfaces, on page 11](#)

## Prerequisites for Configuring Management Ethernet Interfaces

Before you perform the Management Ethernet interface configuration procedures that are described in this chapter, ensure that you meet the following tasks and conditions:

- You have performed the initial configuration of the Management Ethernet interface.
- You know how to apply the generalized interface name specification *rack/slot/module/port*.



---

**Note** For transparent switchover, ensure that both the active and standby Management Ethernet interfaces are physically connected to the same LAN or switch.

---

# Information About Configuring Management Ethernet Interfaces

To configure Management Ethernet interfaces, you must understand the following concept(s):

## Default Interface Settings

This table describes the default Management Ethernet interface settings that you can change with manual configuration. The system does not display the default settings in the **show running-config** command output.

**Table 3: Management Ethernet Interface Default Settings**

Parameter	Default Value	Configuration File Entry
Speed in Mbps	Default speed is <b>1G</b> with autonegotiated.	Speed is non-configurable.
Duplex mode	Default duplex mode is <b>full-duplex</b> with autonegotiated.	Duplex mode is non-configurable.
MAC address	MAC address is read from the hardware burned-in address (BIA).	MAC address is non-configurable.

## How to Perform Advanced Management Ethernet Interface Configuration

This section contains the following procedures:

### Configure a Management Ethernet Interface

Perform this task to configure a Management Ethernet interface. This procedure provides the minimal configuration that is required for the Management Ethernet interface.



**Note** The maximum MTU value for the management interface MgmtEth0/RP0/CPU0/0 is 9678 bytes.

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

/* Enter interface configuration mode and specify the Ethernet interface name and notation
  rack/slot/module/port. */
RP/0/RP0/CPU0:router (config) # interface MgmtEth 0/RP0/CPU0/0

RP/0/RP0/CPU0:router (config-if) # ipv4 address 1.76.18.150/16 (or)
ipv4 address 1.76.18.150 255.255.0.0
```

Assigns an IP address and subnet mask to the interface.

- Replace *ip-address* with the primary IPv4 address for the interface.

- Replace *mask* with the mask for the associated IP subnet. You can specify the network mask in either of the two ways:
- The network mask can be a four-part dotted decimal address. For example, 255.255.0.0 indicates that each bit equal to 1 means that the corresponding address bit belongs to the network address.
- The system indicates the network mask as a slash (/) and number. For example, /16 indicates that the first 16 bits of the mask are ones, and the corresponding bits of the address are the network address.

```
RP/0/RP0/CPU0:router(config-if)# mtu 1488
```



**Note** (Optional) The maximum transmission unit (MTU) value for the management interface is 9678 bytes.

- The default is 1514 bytes.
- The range for the Management Ethernet interface Interface **mtu** values is from 64 through 9678 bytes.

```
/* Remove the shutdown configuration, which removes the forced administrative down on the
interface, enabling it to move to an up or down state. */
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# end
or
RP/0/RP0/CPU0:router(config-if)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

```
RP/0/RP0/CPU0:router# show interfaces MgmtEth 0/RP0/CPU0/0
```

This example displays advanced configuration and verification of the Management Ethernet interface on the RP:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config)# ipv4 address 1.76.18.150/16
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit
```

```
RP/0/RP0/CPU0:router:Mar 26 01:09:28.685 :ifmgr[190]:%LINK-3-UPDOWN :Interface
MgmtEth0/RP0/CPU0/0, changed state to Up
RP/0/RP0/CPU0:router(config-if)# end
```

```
RP/0/RP0/CPU0:router# show interfaces MgmtEth 0/RP0/CPU0/0
```

```
MgmtEth0/RP0/CPU0/0 is up, line protocol is up
Interface state transitions: 3
Hardware is Management Ethernet, address is 1005.cad8.4354 (bia 1005.cad8.4354)
Internet address is 1.76.18.150/16
MTU 1488 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
  reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 1000Mb/s, 1000BASE-T, link type is autonegotiation
loopback not set,
Last link flapped 00:00:59
ARP type ARPA, ARP timeout 04:00:00
Last input 00:00:00, output 00:00:02
Last clearing of "show interface" counters never
5 minute input rate 4000 bits/sec, 3 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  21826 packets input, 4987886 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
  Received 12450 broadcast packets, 8800 multicast packets
    0 runts, 0 giants, 0 throttles, 0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  1192 packets output, 217483 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets
  0 output errors, 0 underruns, 0 applique, 0 resets
  0 output buffer failures, 0 output buffers swapped out
  3 carrier transitions
```

```
RP/0/RP0/CPU0:router# show running-config interface MgmtEth 0/RP0/CPU0/0
```

```
interface MgmtEth0/RP0/CPU0/0
  mtu 1488
  ipv4 address 1.76.18.150/16
  ipv6 address 2002::14c:125a/64
  ipv6 enable
!
```

The following example displays VRF configuration and verification of the Management Ethernet interface on the RP with the source address:

```
RP/0/RP0/CPU0:router# show run interface MgmtEth 0/RP0/CPU0/0
interface MgmtEth0/RP0/CPU0/0
  vrf httpupload
  ipv4 address 10.8.67.20 255.255.0.0
  ipv6 address 2001:10:8:67::20/48
!
```

```
RP/0/RP0/CPU0:router# show run http
Wed Jan 30 14:58:53.458 UTC
http client vrf httpupload
http client source-interface ipv4 MgmtEth0/RP0/CPU0/0
```

```
RP/0/RP0/CPU0:router# show run vrf
Wed Jan 30 14:59:00.014 UTC
vrf httpupload
!
```



## Verify Management Ethernet Interface Configuration

Perform this task to verify configuration modifications on the Management Ethernet interfaces.

```
RP/0/RP0/CPU0:router# show interfaces MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router# show running-config interface MgmtEth 0/RP0/CPU0/0
```

## Configuration Examples for Management Ethernet Interfaces

This section provides the following configuration examples:

### Configuring a Management Ethernet Interface: Example

This example displays advanced configuration and verification of the Management Ethernet interface on the RP:

```
RP/0//CPU0:router# configure
RP/0//CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
RP/0//CPU0:router(config)# ipv4 address 172.29.52.70 255.255.255.0
RP/0//CPU0:router(config-if)# no shutdown
RP/0//CPU0:router(config-if)# commit
RP/0//CPU0:Mar 26 01:09:28.685 :ifmgr[190]:%LINK-3-UPDOWN :Interface MgmtEth 0/RP0/CPU0/0,
  changed state to Up
RP/0//CPU0:router(config-if)# end

RP/0//CPU0:router# show interfaces MgmtEth 0/RP0/CPU0/0

MMgmtEth0//CPU0/0 is up, line protocol is up
  Hardware is Management Ethernet, address is 0011.93ef.e8ea (bia 0011.93ef.e8ea
)
  Description: Connected to Lab LAN
  Internet address is 172.29.52.70/24
  MTU 1514 bytes, BW 100000 Kbit
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 3000 bits/sec, 7 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
    30445 packets input, 1839328 bytes, 64 total input drops
    0 drops for unrecognized upper-level protocol
    Received 23564 broadcast packets, 0 multicast packets
      0 runts, 0 giants, 0 throttles, 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  171672 packets output, 8029024 bytes, 0 total output drops
  Output 16 broadcast packets, 0 multicast packets
  0 output errors, 0 underruns, 0 applique, 0 resets
  0 output buffer failures, 0 output buffers swapped out
  1 carrier transitions

RP/0//CPU0:router# show running-config interface MgmtEth 0/

interface MgmtEth0/RP0/CPU0/0
  description Connected to Lab LAN
```

```
ipv4 address 172.29.52.70 255.255.255.0  
!
```



## CHAPTER 4

# Configuring Ethernet Interfaces

This module describes the configuration of Ethernet interfaces.

The distributed 10-Gigabit, 40-Gigabit, 100-Gigabit Ethernet, 400-Gigabit Ethernet architecture and features deliver network scalability and performance, while enabling service providers to offer high-density, high-bandwidth networking solutions designed to interconnect the router with other systems in POPs, including core and edge routers, Layer 2 switches and Layer 3 switches.

**Table 4: Feature History Table**

Feature Name	Release Information	Feature Description
Introduction of IP MTU on Q200-based Systems	Release 7.5.2	You can configure IP MTU for IPv4 and IPv6 on a Layer 3 interface. Depending on your specific network requirements, this ability to specify IP MTU settings helps optimize router data transmission.  Use the <code>show ipv4/ipv6 interfaces</code> command to view the IP MTU configurations.



**Tip** You can programmatically configure and manage the Ethernet interfaces using `openconfig-if-ethernet.yang` and `openconfig-interfaces.yang` OpenConfig data models. To get started with using data models, see the *Programmability Configuration Guide for Cisco 8000 Series Routers*.

- [Prerequisites for Configuring Ethernet Interfaces, on page 14](#)
- [Information About Configuring Ethernet, on page 14](#)
- [Setting the Carrier Delay on Physical Interfaces, on page 36](#)
- [How to Configure Ethernet, on page 37](#)
- [Viewing Interface Counters Report, on page 51](#)
- [How to Configure Interfaces in Breakout Mode, on page 53](#)

## Prerequisites for Configuring Ethernet Interfaces

Before configuring Ethernet interfaces, ensure that you meet the following conditions:

- Access to Cisco 8200 series routers or Cisco 8800 series routers with at least one of the supported line cards installed.
- Know the interface IP address.
- Ensure to specify the generalized interface name with the standard notation of *rack/slot/module/port*.

## Information About Configuring Ethernet

This section provides the following information:

### Cisco 8000 Modular Line Cards

The current release of the Cisco 8800 Series Routers support the following line cards:

- 36-port QSFP56-DD 400 GbE Line Card - This line card provides 14.4 Tbps via 36 QSFP56-DD ports. It also supports 100G, 2x100G, and 400G modules. If 36 of 2x100G modules are used, the line card can have 72 HundredGigE interfaces.
- 48-port QSFP28 100 GbE Line Card - This line card provides 4.8 Tbps with MACsec support on all ports. It also supports QSFP+ optics for 40G compatibility.

The 8800 Series line cards utilize multiple #ChipName forwarding ASICs to achieve high performance and bandwidth with line rate forwarding.

### Default Configuration Values for 100-Gigabit Ethernet

This table describes the default interface configuration parameters that are present when an interface is enabled on a 36-port Line Card or a 48-port Line Card.



**Note** You must use the **shutdown** command to bring an interface administratively down. The interface default is **no shutdown**. When a line card is first inserted into the router, if there is no established preconfiguration for it, the configuration manager adds a shutdown item to its configuration. This shutdown can be removed only by entering the **no shutdown** command.

*Table 5: 100-Gigabit Ethernet Line Card Default Configuration Values*

Parameter	Configuration File Entry	Default Value
Flow control	<b>flow-control</b>	egress off ingress off

Parameter	Configuration File Entry	Default Value
MTU	<b>mtu</b>	<ul style="list-style-type: none"> <li>• 1514 bytes for normal frames</li> <li>• 1518 bytes for 802.1Q tagged frames.</li> <li>• 1522 bytes for Q-in-Q frames.</li> </ul>
MAC address	<b>mac address</b>	Hardware burned-in address (BIA)

## Layer 2 VPN on Ethernet Interfaces

Layer 2 Virtual Private Network (L2VPN) connections emulate the behavior of a LAN across an L2 switched, IP or MPLS-enabled IP network, allowing Ethernet devices to communicate with each other as if they were connected to a common LAN segment.

The L2VPN feature enables service providers (SPs) to provide Layer 2 services to geographically disparate customer sites. Typically, an SP uses an access network to connect the customer to the core network. On the router, this access network is typically Ethernet.

Traffic from the customer travels over this link to the edge of the SP core network. The traffic then tunnels through an L2VPN over the SP core network to another edge router. The edge router sends the traffic down another attachment circuit (AC) to the customer's remote site.

On the router, an AC is an interface that is attached to an L2VPN component, such as a bridge domain.

The L2VPN feature enables users to implement different types of end-to-end services.

Switching takes place through local switching where traffic arriving on one AC is immediately sent out of another AC without passing through a pseudowire.

Keep the following in mind when configuring L2VPN on an Ethernet interface:

- L2VPN links support QoS (Quality of Service) and MTU (maximum transmission unit) configuration.
- If your network requires that packets are transported transparently, you may need to modify the packet's destination MAC (Media Access Control) address at the edge of the Service Provider (SP) network. This prevents the packet from being consumed by the devices in the SP network.

Use the **show interfaces** command to display AC information.

To attach Layer 2 service policies, such as QoS, to the Ethernet interface, refer to the appropriate Cisco IOS XR software configuration guide.

## Gigabit Ethernet Protocol Standards Overview

The Gigabit Ethernet interfaces support the following protocol standards:

These standards are further described in the sections that follow.

## IEEE 802.3 Physical Ethernet Infrastructure

The IEEE 802.3 protocol standards define the physical layer and MAC sublayer of the data link layer of wired Ethernet. IEEE 802.3 uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access at various speeds over various physical media. The IEEE 802.3 standard covers 10 Mbps Ethernet. Extensions to the IEEE 802.3 standard specify implementations for 40-Gigabit Ethernet and 100-Gigabit Ethernet.

### IEEE 802.3ae 10-Gbps Ethernet

Under the International Standards Organization's Open Systems Interconnection (OSI) model, Ethernet is fundamentally a Layer 2 protocol. 10-Gigabit Ethernet uses the IEEE 802.3 Ethernet MAC protocol, the IEEE 802.3 Ethernet frame format, and the minimum and maximum IEEE 802.3 frame size. 10-Gbps Ethernet conforms to the IEEE 802.3ae protocol standards.

Just as 1000BASE-X and 1000BASE-T (Gigabit Ethernet) remained true to the Ethernet model, 10-Gigabit Ethernet continues the natural evolution of Ethernet in speed and distance. Because it is a full-duplex only and fiber-only technology, it does not need the carrier-sensing multiple-access with the CSMA/CD protocol that defines slower, half-duplex Ethernet technologies. In every other respect, 10-Gigabit Ethernet remains true to the original Ethernet model.

### IEEE 802.3ba 100 Gbps Ethernet

IEEE 802.3ba is supported on the Cisco 1-Port 100-Gigabit Ethernet PLIM beginning in Cisco IOS XR 7.0.11.

## MAC Address

A MAC address is a unique 6-byte address that identifies the interface at Layer 2.

## Ethernet MTU

The Ethernet maximum transmission unit (MTU) is the size of the largest frame, minus the 4-byte frame check sequence (FCS), that the system transmits on the Ethernet network. Every physical network along the destination of a packet can have a different MTU.

Cisco IOS XR software supports two types of frame forwarding processes:

- Fragmentation for IPv4 packets – In this process, IPv4 packets are fragmented as necessary to fit within the MTU of the next-hop physical network.




---

**Note** IPv6 does not support fragmentation.

---

- MTU discovery process determines largest packet size – This process is available for all IPv6 devices, and for originating IPv4 devices. In this process, the originating IP device determines the size of the largest IPv6 or IPv4 unfragmented packet that the system can send. The largest packet is equal to the smallest MTU of any network between the IP source and the IP destination devices. If a packet is larger than the smallest MTU of all the networks in its path, the system fragments that packet as necessary. This process ensures that the originating device does not send an IP packet that is too large.

The system automatically enables the jumbo frame support for frames that exceed the standard frame size. The default value is 1514 for standard frames and 1518 for 802.1Q tagged frames. These numbers exclude the 4-byte frame check sequence (FCS).

## IP MTU

In IP protocol, Maximum Transmission Unit (MTU) refers to the maximum size of an IP packet that the system transmits without fragmentation over a given medium. The size of an IP packet includes IP headers but excludes headers from the data link layer, also known as the Ethernet headers. The default IP MTU on all router interfaces is 1500 bytes, when IP is enabled by using the IP address configuration commands. However, you can configure the IP MTU to different value as well.

Starting Cisco IOS XR Release 7.5.2, the system supports IP MTU (IPv4 and IPv6) on Q200-based systems on the following Cisco 8000 Series router and line card:

- 8201-32FH
- 88-LC0-36FH-M

### How is Ethernet MTU different from IP MTU?

Ethernet MTU defines the maximum packet size that an interface supports, while IP MTU defines the MTU size of an IP packet.

### How is IP MTU calculated?

The following scenarios provide information on how the system calculates IP MTU size, when:

- Ethernet MTU is not configured, the system sets:
  - Default value as 1514 bytes on a physical or bundle main interface
  - 1518 bytes for single tag VLAN interface
  - 1522 bytes for double tag VLAN (QinQ) interface




---

**Note** In this case, IP MTU value will be 1500 bytes for IPv4 and IPv6 MTUs.

---

- Ethernet MTU is configured as X bytes, the system sets:
  - X bytes on a physical or bundle main interface
  - X+4 bytes for single tag VLAN interface
  - X+8 bytes for double tag VLAN (QinQ) interface




---

**Note** In this case, IP MTU is X-14 bytes for IPv4 and IPv6 MTUs.

---

The following are some of the important guidelines for IP MTU size:

- When no Ethernet MTU and IP MTU is configured, the default value is 1500B.

- When Ethernet MTU and no IP MTU is configured, IP MTU value in the hardware is Ethernet MTU-14B.
- IP MTU value can't be more than Ethernet MTU value. For example, if the Ethernet MTU value is 3000 bytes and you configure IP MTU value as 5000 bytes. The system sets the IP MTU value as 2986 (3000-14)

### What is Maximum Receive Unit (MRU) and how is it different from MTU?

MRU is the largest packet size that an interface can receive. This is an ingress parameter. Usually, MRU equals MTU. However, you can't configure an MRU value. The Ethernet MTU, also known as a Layer2 (L2) value that you configure on a physical interface is also applied as the MRU of that physical interface.

The following table lists Ethernet MTU, IPv4, and IPv6 MTU support across various platforms and their limitations as applicable:

**Table 6: IP MTU Support Across Platforms**

ASIC	Ethernet MTU Check	IPv4 and IPv6 MTU
Q100-based	Ethernet MTU check on an egress interface is not supported.	Supported and the system derives IP MTU value from Ethernet MTU.
Q200-based	Ethernet MTU check on an egress interface is not supported.	Supported <b>Note</b> IPv4 and IPv6 can have their own separate MTU values.

## IP MTU Checks

Cisco IOS XR supports MRU checks, ethernet MTU checks, and IP MTU checks. These checks decide if an IP payload packets needs fragmentation or not. Ethernet MTU and IP MTU check is applied on all egress traffic for each packet that flows in the system. In the forwarding plane, also known as dataplane, the IP packet length is compared against IP MTU value applied on the L3 forwarding interface. Full packet length is compared against ethernet MTU value applied on the physical port.

The following table describes IP MTU check to each forwarding flow on Q200-based and Q100-based systems.

**Table 7: IP MTU Check**

ASIC	IP MTU Check
Q100-based	These interfaces implement IP MTU checks and provide fragmentation for all IP payload packets. A single value for both IPv4 and IPv6 is supported.
Q200-based	These interfaces implement IP MTU checks and provide fragmentation for all IP payload packets.
Mixed System with Q100 and Q200-based line cards	Interfaces with Q100-based system provides its behavior and interfaces with Q200-based systems provides its behavior as described in this table.



## IP MTU Configuration Guidelines

An Ethernet interface has a default of 1514 bytes. IP MTU is always derived from the default Ethernet MTU. If Ethernet MTU is configured, IP MTU is derived from the previously configured Ethernet MTU.

The following are the configuration guidelines for IP MTU across various platforms:

### Guidelines for Q200-based Systems

- If you don't define any Ethernet MTU configuration, the system assigns the default value of Ethernet packet size of 1514 bytes.
- For IPv4 and IPv6 MTUs, 1500 bytes is used, which is derived by subtracting 14 bytes of Ethernet header size from its default value.
- On any interface, if an Ethernet MTU is configured, the new configuration takes higher precedence than the default interface configuration. However, in such a scenario, the new configuration doesn't get applied on the subinterfaces. The rest of the interfaces continue to work with the default Ethernet MTU configurations.
- For the double tag (QinQ) packets, MRU and Ethernet MTU value are derived by adding 8 bytes to the configured value.
- IPv4 and IPv6 MTU values are derived by subtracting 14 bytes of the Ethernet header size out of the configured value.
- If an IPv4 or IPv6 MTU is configured, it is applied to IP MTU value. MRU or MTU values remain unaffected by this configuration.
- Configuration restrictions apply to validate that the IP MTU value is smaller than Ethernet MTU value that is configured on an interface.

The following sample table explains how the system calculates the Ethernet MTU, IPv4, and IPv6 MTU values when configured on various interfaces that are Q200-based systems.

**Table 8: Interfaces and Configurations**

<b>Interface Type</b>	<b>Default Configurations when, no Ethernet or IP MTU configuration is applied</b>	<b>Ethernet MTU Configurations for example, MTU = 1614</b>	<b>IPv4/IPv6 Configurations for example, IPv4   IPv6 MTU = 1550, Ethernet MTU = 1614</b>
Any Main Interface	NA	Configuration that is applied on any main interface and its subinterfaces is effective.  Configuration that is applied on any subinterface is not effective.	NA
Physical Port	MRU = 1514 + 8	MRU = 1614 + 8	MRU = 1614 + 8

Interface Type	Default Configurations <i>when, no Ethernet or IP MTU configuration is applied</i>	Ethernet MTU Configurations <i>for example, MTU = 1614</i>	IPv4/IPv6 Configurations <i>for example, IPv4   IPv6 MTU = 1550, Ethernet MTU = 1614</i>
L3 Main Interface (Physical or bundle)	Ethernet MTU = 1514 + 8  IPv4/IPv6 MTU = 1500	Ethernet MTU = 1614 + 8  IPv4/IPv6 MTU = 1614 - 14	Ethernet MTU = 1614 + 8  IPv4/IPv6 MTU = 1550
L3 Sub-interface (Physical or bundle)	Ethernet MTU = 1514 + 8  IPv4/IPv6 MTU = 1500	<b>Note</b> Configuration not applicable on subinterfaces. Takes main interface configuration.  Ethernet MTU = Not applicable  IPv4/IPv6 MTU = 1614 - 14	Ethernet MTU = 1614 + 8  IPv4/IPv6 MTU = 1550
SVI/BVI	IPv4/IPv6 MTU = 1500	Ethernet MTU = Not applicable  IPv4/IPv6 MTU = 1600	IPv4/IPv6 MTU = 1550
Ethernet Main Interface	Ethernet MTU = 1514 + 8	Ethernet MTU = 1614 + 8  IPv4/IPv6 MTU = Not applicable	Not applicable  Ethernet MTU = 1614 + 8
Ethernet Sub-interface	Ethernet MTU = 1514 + 8	Ethernet MTU = 1614 + 8  IPv4/IPv6 MTU = Not applicable	Not applicable  Ethernet MTU = 1614 + 8

### Guidelines for Q100-based Systems

- If you don't define any MTU configuration in the system, the system assigns default value of 1514 bytes to the Ethernet packets.
- An MRU of 1522 bytes is set to allow for any double tag packets on an interface.
- Ethernet MTU check on egress interface is not supported.
- For IPv4 and IPv6 MTUs, 1500 bytes is used, which is derived by subtracting 14 bytes of Ethernet header size from its default value.

- If you configure an IP MTU (IPv4/IPv6 MTU) on any interface, the configuration does not take effect.

The following table lists the MTU configurations and MTU calculations on various interfaces for Q100-based systems:

**Table 9: Interfaces and Configurations**

Interface Type	Default Configurations	Interface MTU Configurations <i>where, MTU = 1614</i>
Any Main Interface	NA	Configuration applied on any main interface and its subinterfaces is effective.  Configuration applied on any sub-interface is not effective.
Physical Port	MRU = 1514 + 8	MRU = 1614 + 8
L3 Main Interface (Physical or bundle)	Ethernet MTU check on egress interface is not supported.  IPv4/IPv6 MTU = 1522 applied on full packet size	Ethernet MTU check on egress interface is not supported.  IPv4/IPv6 MTU = 1622 applied on full packet size
L3 Subinterface (Physical or bundle)	Ethernet MTU check on egress interface is not supported.  IPv4/IPv6 MTU = 1522 applied on full packet size	<b>Note</b> Configuration not applicable on sub-interfaces. Takes main interface configuration.  Ethernet MTU = Not applicable  IPv4/IPv6 MTU = 1622 applied on full packet size
SVI and BVI	Ethernet MTU is not applicable  IPv4/IPv6 MTU = 1522 applied on full packet size	
Ethernet Main Interface	Ethernet MTU check on egress interface is not supported.  IPv4/IPv6 MTU is not applicable	
Ethernet Subinterface	Ethernet MTU check on egress interface is not supported.  IPv4/IPv6 MTU is not applicable	
GRE tunnel	Ethernet MTU check on egress interface is not supported.  IPv4/IPv6 MTU = 1522 applied on full packet size	

## IP MTU Limitations and Feature Support

The following are the limitations and feature support for IP MTU:

- MPLS MTU is not supported.
- GRE/IPinIP MTU is not supported.
- Multicast MDT MTU is not supported.
- Ethernet MTU configuration on sub-interfaces is not supported.
- Ethernet MTU configuration on BVI interfaces is not supported.




---

**Important** Although CLIs for the unsupported features might be available on your router, they are not functional.

---

## IP MTU Scale

The following are the scale support and limitations for IP MTU configurations:

- Ethernet MTU configuration is allowed on every physical or bundle interface without any scale limits.
- IPv4/IPv6 MTU configuration is allowed on every L3 forwarding interface. However, the system applies it as an IP MTU profile with a combination of <IPv4 MTU and IPv6 MTU> set. Each profile takes a unique set of these two MTUs, and supports eight such unique MTUs. The IP MTU profiles are stored identically across all NPUs of a given line card.
- When system runs out of resources (OOR), the system generates syslog messages while the continuing to use the previously configured IP MTU values.

## Configure IP MTU

To configure IPv4, or IPv6 MTU, you must be in the configuration mode on L3 interface.

To configure IP MTU, use the following configuration steps:

```
Router#config t
Router#interface HundredGigE0/0/0/33
Router:abc(config)#
Router:abc(config-if)#ipv4 mtu 2000
Router:abc(config-subif)#commit
Router:abc(config-if)#end
```

### Running Configuration

```
Router:abc#
Router:abc#sh ipv4 int HundredGigE0/0/0/33
Thu Apr 28 16:54:10.820 UTC
HundredGigE0/0/0/33 is Shutdown, ipv4 protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet address is 10.10.10.91/29
  MTU is 9642 (2000 is available to IP)
```

**Verification**

```

Router:abc#sh int HundredGigE0/0/0/33
Thu Apr 28 16:57:23.390 UTC
HundredGigE0/0/0/33 is administratively down, line protocol is administratively down
  Interface state transitions: 0
  Hardware is HundredGigE, address is e41f.7bde.123c (bia e41f.7bde.123c)
  Internet address is 194.19.242.94/29
  MTU 9642 bytes, BW 100000000 Kbit (Max: 100000000 Kbit)
    reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 100000Mb/s, 100GBASE-AOC, link type is force-up
  output flow control is off, input flow control is off
  Carrier delay (up) is 10 msec
  loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
  Last input never, output never
  Last clearing of "show interface" counters never
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
  Received 0 broadcast packets, 0 multicast packets
    0 runts, 0 giants, 0 throttles, 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets
    0 output errors, 0 underruns, 0 applique, 0 resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions

```

```
Router:abc#
```

**Configure IPv4 MTU**

To configure IPv4 MTU, use the following configuration steps:

```

Router#config t
Router#interface HundredGigE0/0/0/33
Router:abc(config)#
Router:abc(config-if)#ipv4 mtu 2000
Router:abc(config-subif)#commit
Router:abc(config-if)#end

```

**Running Configuration**

```

Router:abc#sh run int HundredGigE0/0/0/33
Thu Apr 28 16:22:06.796 UTC
interface HundredGigE0/0/0/33
mtu 9642
ipv4 mtu 2000
ipv4 address 10.10.10.1 255.255.255.248
ipv6 address 10::1:10:9/112
load-interval 30
!

```

**Verification**

```
Router:abc#sh ipv4 int HundredGigE0/0/0/33
Thu Apr 28 16:54:10.820 UTC
HundredGigE0/0/0/33 is Shutdown, ipv4 protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet address is 10.10.10.1/29
  MTU is 9642 (2000 is available to IP)
```

**Configure IPv6 MTU**

To configure IPv6 MTU, use the following configuration steps:

```
Router#config t
Router#interface HundredGigE0/0/0/33
Router:abc(config)#
Router:abc(config-if)#ipv6 mtu 3000
Router:abc(config-subif)#commit
Router:abc(config-if)#end
```

**Running Configuration**

```
Router:abc#sh run int HundredGigE0/0/0/33
Thu Apr 28 16:23:09.141 UTC
interface HundredGigE0/0/0/33
mtu 9642
ipv4 mtu 2000
ipv4 address 10.10.10.1 255.255.255.248
ipv6 mtu 3000
ipv6 address 10::10:10:9/112
load-interval 30
!

Router:abc#
```

**Verification**

```
Router:abc#sh ipv6 int HundredGigE0/0/0/33
Thu Apr 28 16:54:41.222 UTC
HundredGigE0/0/0/33 is Shutdown, ipv6 protocol is Down, Vrfid is default (0x60000000)
  IPV6 is enabled, link-local address is fe80::e61f:7bff:fede:123c [TENTATIVE]
  Global unicast address(es):
    194::19:242:94, subnet is 10::10:10:0/112 [TENTATIVE]
  Joined group address(es): ff02::2 ff02::1
  MTU is 9642 (3000 is available to IPv6)
```

## Flow Control on Ethernet Interfaces

The flow control that the system uses on 10-Gigabit Ethernet interfaces consists of periodically sending flow control pause frames. It is fundamentally different from the usual full and half-duplex flow control that is used on standard management interfaces. You can activate or deactivate flow control for ingress traffic only. The system automatically implements flow control for egress traffic.

## 802.1Q VLAN

A VLAN is a group of devices on one or more LANs that the system configures so that they can communicate as if they are attached to the same wire, when in fact they are located on several different LAN segments. Because VLANs are based on logical instead of physical connections, it is flexible for user and host management, bandwidth allocation, and resource optimization.

The IEEE's 802.1Q protocol standard addresses the problem of breaking large networks into smaller parts so broadcast and multicast traffic does not consume more bandwidth than necessary. The standard also helps to provide a higher level of security between segments of internal networks.

The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames.

## Subinterfaces on the Router

In Cisco IOS XR, interfaces are, by default, main interfaces. A main interface is also known as a trunk interface, which you must not confuse with the word trunk in the context of VLAN trunking.

There are two types of trunk interfaces:

- Physical
- Bundle

On the router, the system automatically creates the physical interfaces when the router recognizes a card and its physical interfaces. However, the system does not automatically create bundle interfaces but you must create them at the time of configuration.

The following configuration samples are examples of the trunk interfaces that you can create:

- interface HundredGigE 0/5/0/0
- interface bundle-ether 1

A subinterface is a logical interface that the system create under a trunk interface.

To create a subinterface, you must first identify a trunk interface under which to place it. In case of bundle interfaces, if a trunk interface does not exist, you must create a bundle interface before creating any subinterfaces under it.

You can then assign a subinterface number to the subinterface that you want to create. The subinterface number must be a positive integer from zero to some high value. For a given trunk interface, each subinterface under it must have a unique value.

Subinterface numbers do not need to be contiguous or in numeric order. For example, the following subinterfaces numbers are valid under one trunk interface:

1001, 0, 97, 96, 100000

Subinterfaces can never have the same subinterface number under one trunk.

In the following example, the card in slot 5 has trunk interface, HundredGigE 0/5/0/0. A subinterface, HundredGigE 0/5/0/0.0, is created under it.

```
RP/0/RSP0/CPU0:router# conf
Mon Sep 21 11:12:11.722 EDT
RP/0/RSP0/CPU0:router(config)# interface HundredGigE0/5/0/0.0
```

```

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

RP/0/RSP0/CPU0:Sep 21 11:12:34.819 : config[65794]: %MGBL-CONFIG-6-DB_COMMIT : Configuration
  committed by user 'root'. Use 'show configuration commit changes 1000000152' to view the
  changes.

RP/0/RSP0/CPU0:router(config-subif)# end

RP/0/RSP0/CPU0:Sep 21 11:12:35.633 : config[65794]: %MGBL-SYS-5-CONFIG_I : Configured from
  console by root
RP/0/RSP0/CPU0:router#

```

The **show run** command displays the trunk interface first, then the subinterfaces in ascending numerical order.

```

RP/0/RSP0/CPU0:router# show run | begin HundredGigE 0/5/0/0
Mon Sep 21 11:15:42.654 EDT
Building configuration...
interface HundredGigE 0/5/0/0
  shutdown
!
interface HundredGigE 0/5/0/0.0
  encapsulation dot1q 100
!
interface HundredGigE 0/5/0/1
  shutdown
!

```

When a subinterface is first created, the router recognizes it as an interface that, with few exceptions, is interchangeable with a trunk interface. After the new subinterface is configured further, the **show interface** command can display it along with its unique counters:

The following example shows the display output for the trunk interface, HundredGigE 0/5/0/0, followed by the display output for the subinterface HundredGigE 0/5/0/0.0.

```

RP/0/RSP0/CPU0:router# show interface HundredGigE 0/5/0/0
Mon Sep 21 11:12:51.068 EDT
HundredGigE0/5/0/0 is administratively down, line protocol is administratively down.
  Interface state transitions: 0
  Hardware is HundredGigE, address is 0024.f71b.0ca8 (bia 0024.f71b.0ca8)
  Internet address is Unknown
  MTU 1514 bytes, BW 1000000 Kbit
    reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation 802.1Q Virtual LAN,
  Full-duplex, 1000Mb/s, SXFD, link type is force-up
  output flow control is off, input flow control is off
  loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
  Last input never, output never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
  Received 0 broadcast packets, 0 multicast packets
    0 runts, 0 giants, 0 throttles, 0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets
  0 output errors, 0 underruns, 0 applique, 0 resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions

```



```
RP/0/RSP0/CPU0:router# show interface HundredGigE0/5/0/0.0
Mon Sep 21 11:12:55.657 EDT
HundredGigE0/5/0/0.0 is administratively down, line protocol is administratively down.
  Interface state transitions: 0
  Hardware is VLAN sub-interface(s), address is 0024.f71b.0ca8
  Internet address is Unknown
  MTU 1518 bytes, BW 1000000 Kbit
    reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation 802.1Q Virtual LAN, VLAN Id 100, loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
  Last input never, output never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
  Received 0 broadcast packets, 0 multicast packets
  0 packets output, 0 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets
```

This example shows two interfaces being created at the same time: first, the bundle trunk interface, then a subinterface attached to the trunk:

```
RP/0/RSP0/CPU0:router# conf
Mon Sep 21 10:57:31.736 EDT
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether1
RP/0/RSP0/CPU0:router(config-if)# no shut
RP/0/RSP0/CPU0:router(config-if)# interface bundle-Ether1.0
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 100
RP/0/RSP0/CPU0:router(config-subif)# commit
RP/0/RSP0/CPU0:Sep 21 10:58:15.305 : config[65794]: %MGBL-CONFIG-6-DB_COMMIT : C
onfiguration committed by user 'root'. Use 'show configuration commit changes 10
00000149' to view the changes.
RP/0/RSP0/CPU0:router# show run | begin Bundle-Ether1
Mon Sep 21 10:59:31.317 EDT
Building configuration..
interface Bundle-Ether1
!
interface Bundle-Ether1.0
  encapsulation dot1q 100
!
```

You delete a subinterface using the **no interface** command.

```
RP/0/RSP0/CPU0:router#
RP/0/RSP0/CPU0:router# show run | begin HundredGigE 0/5/0/0
Mon Sep 21 11:42:27.100 EDT
Building configuration...
interface HundredGigE 0/5/0/0
  negotiation auto
!
interface HundredGigE 0/5/0/0.0
  encapsulation dot1q 100
!
interface HundredGigE 0/5/0/1
  shutdown
!
RP/0/RSP0/CPU0:router# conf
Mon Sep 21 11:42:32.374 EDT
RP/0/RSP0/CPU0:router(config)# no interface HundredGigE 0/5/0/0.0
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:Sep 21 11:42:47.237 : config[65794]: %MGBL-CONFIG-6-DB_COMMIT : Configuration
```

```

    committed by user 'root'. Use 'show configuration commit changes 1000000159' to view the
    changes.
RP/0/RSP0/CPU0:router(config)# end
RP/0/RSP0/CPU0:Sep 21 11:42:50.278 : config[65794]: %MGBL-SYS-5-CONFIG_I : Configured from
    console by root
RP/0/RSP0/CPU0:router# show run | begin HundredGigE 0/5/0/0
Mon Sep 21 11:42:57.262 EDT
Building configuration...
interface HundredGigE 0/5/0/0
    negotiation auto
!
interface HundredGigE 0/5/0/1
    shutdown
!

```

## Layer 2, Layer 3, and EFPs

On the router, a trunk interface can be either a Layer 2 or Layer 3 interface. A Layer 2 interface is configured using the **interface** command with the **l2transport** keyword. When the **l2transport** keyword is not used, the interface is a Layer 3 interface. Subinterfaces are configured as Layer 2 or Layer 3 subinterface in the same way.

A Layer 3 trunk interface or subinterface is a routed interface and can be assigned an IP address. Traffic sent on that interface is routed.

A Layer 2 trunk interface or subinterface is a switched interface and cannot be assigned an IP address. A Layer 2 interface must be connected to an L2VPN component. Once it is connected, it is called an access connection.

Subinterfaces can only be created under a Layer 3 trunk interface. Subinterfaces cannot be created under a Layer 2 trunk interface.

A Layer 3 trunk interface can have any combination of Layer 2 and Layer 3 interfaces.

The following example shows an attempt to configure a subinterface under an Layer 2 trunk and the commit errors that occur. It also shows an attempt to change the Layer 2 trunk interface to an Layer 3 interface and the errors that occur because the interface already had an IP address assigned to it.

```

RP/0/RP0/CPU0:router# config
Mon Sep 21 12:05:33.142 EDT
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/5/0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.0.1/24
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:Sep 21 12:05:57.824 : config[65794]: %MGBL-CONFIG-6-DB_COMMIT : Configuration
    committed by user 'root'. Use 'show configuration commit changes 1000000160' to view the
    changes.
RP/0/RP0/CPU0:router(config-if)# end
RP/0/RP0/CPU0:Sep 21 12:06:01.890 : config[65794]: %MGBL-SYS-5-CONFIG_I : Configured from
    console by root
RP/0/RP0/CPU0:router# show run | begin HundredGigE0/5/0/0
Mon Sep 21 12:06:19.535 EDT
Building configuration...
interface HundredGigE0/5/0/0
    ipv4 address 10.0.0.1 255.255.255.0
    negotiation auto
!
interface HundredGigE0/5/0/1
    shutdown
!
RP/0/RP0/CPU0:router#
RP/0/RP0/CPU0:router#

```

```

RP/0/RP0/CPU0:router# conf
Mon Sep 21 12:08:07.426 EDT
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/5/0/0 l2transport
RP/0/RP0/CPU0:router(config-if-l2)# commit

% Failed to commit one or more configuration items during a pseudo-atomic operation. All
changes made have been reverted. Please issue 'show configuration failed' from this session
to view the errors
RP/0/RP0/CPU0:router(config-if-l2)# no ipv4 address
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:Sep 21 12:08:33.686 : config[65794]: %MGBL-CONFIG-6-DB_COMMIT : Configuration
committed by user 'root'. Use 'show configuration commit changes 1000000161' to view the
changes.
RP/0/RP0/CPU0:router(config-if)# end
RP/0/RP0/CPU0:Sep 21 12:08:38.726 : config[65794]: %MGBL-SYS-5-CONFIG_I : Configured from
console by root
RP/0/RP0/CPU0:router#
RP/0/RP0/CPU0:router# show run interface HundredGigE0/5/0/0
Mon Sep 21 12:09:02.471 EDT
interface HundredGigE0/5/0/0
  negotiation auto
  l2transport
  !
!
RP/0/RP0/CPU0:router#
RP/0/RP0/CPU0:router# conf
Mon Sep 21 12:09:08.658 EDT
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/5/0/0.0
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/5/0/0.0
RP/0/RP0/CPU0:router(config-subif)# commit

% Failed to commit one or more configuration items during a pseudo-atomic operation. All
changes made have been reverted. Please issue 'show configuration failed' from this session
to view the errors
RP/0/RP0/CPU0:router(config-subif)#
RP/0/RP0/CPU0:router(config-subif)# interface HundredGigE0/5/0/0
RP/0/RP0/CPU0:router(config-if)# no l2transport
RP/0/RP0/CPU0:router(config-if)# interface HundredGigE0/5/0/0.0
RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 99
RP/0/RP0/CPU0:router(config-subif)# ipv4 address 11.0.0.1/24
RP/0/RP0/CPU0:router(config-subif)# interface HundredGigE0/5/0/0.1 l2transport
RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 700
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:Sep 21 12:11:45.896 : config[65794]: %MGBL-CONFIG-6-DB_COMMIT : Configuration
committed by user 'root'. Use 'show configuration commit changes 1000000162' to view the
changes.
RP/0/RP0/CPU0:router(config-subif)# end
RP/0/RP0/CPU0:Sep 21 12:11:50.133 : config[65794]: %MGBL-SYS-5-CONFIG_I : Configured from
console by root
RP/0/RP0/CPU0:router#
RP/0/RP0/CPU0:router# show run | b HundredGigE0/5/0/0
Mon Sep 21 12:12:00.248 EDT
Building configuration...
interface HundredGigE0/5/0/0
  negotiation auto
  !
interface HundredGigE0/5/0/0.0
  ipv4 address 11.0.0.1 255.255.255.0
  encapsulation dot1q 99
  !
interface HundredGigE0/5/0/0.1 l2transport
  encapsulation dot1q 700
  !

```

```
interface HundredGigE0/5/0/1
 shutdown
 !
```

All subinterfaces must have unique encapsulation statements, so that the router can send incoming packets and frames to the correct subinterface. If a subinterface does not have an encapsulation statement, the router will not send any traffic to it.

In Cisco IOS XR, an Ethernet Flow Point (EFP) is implemented as a Layer 2 subinterface, and consequently, a Layer 2 subinterface is often called an EFP.

A Layer 2 trunk interface can be used as an access connection. However, a Layer 2 trunk interface is not an EFP because an EFP, by definition, is a substream of an overall stream of traffic.

Cisco IOS XR also has other restrictions on what can be configured as a Layer 2 or Layer 3 interface. Certain configuration blocks only accept Layer 3 and not Layer 2. For example, OSPF only accepts Layer 3 trunks and subinterface. Refer to the appropriate Cisco IOS XR configuration guide for other restrictions.

## Enhanced Performance Monitoring for Layer 2 Subinterfaces (EFPs)

Beginning in Cisco IOS XR Release 7.2.12, the router adds support for basic counters for performance monitoring on Layer 2 subinterfaces. This section provides a summary of the new support for Layer 2 interface counters.

The **interface basic-counters** keyword has been added to support a new entity for performance statistics collection and display on Layer 2 interfaces in the following commands:

- **performance-mgmt statistics interface basic-counters**
- **performance-mgmt threshold interface basic-counters**
- **performance-mgmt apply statistics interface basic-counters**
- **performance-mgmt apply threshold interface basic-counters**
- **performance-mgmt apply monitor interface basic-counters**
- **show performance-mgmt monitor interface basic-counters**
- **show performance-mgmt statistics interface basic-counters**

The **performance-mgmt threshold interface basic-counters** command supports the following attribute values for Layer 2 statistics, which also appear in the **show performance-mgmt statistics interface basic-counters** and **show performance-mgmt monitor interface basic-counters** command:

Attribute	Description
InOctets	Bytes received (64-bit)
InPackets	Packets received (64-bit)
InputQueueDrops	Input queue drops (64-bit)
InputTotalDrops	Inbound correct packets discarded (64-bit)
InputTotalErrors	Inbound incorrect packets discarded (64-bit)
OutOctets	Bytes sent (64-bit)

Attribute	Description
OutPackets	Packets sent (64-bit)
OutputQueueDrops	Output queue drops (64-bit)
OutputTotalDrops	Outband correct packets discarded (64-bit)
OutputTotalErrors	Outband incorrect packets discarded (64-bit)

## Other Performance Management Enhancements

The following additional performance management enhancements are included in Cisco IOS XR Release 7.0.11:

- You can retain performance management history statistics across a process restart or route processor (RP) failover using the new **history-persistent** keyword option for the **performance-mgmt statistics interface** command.
- You can save performance management statistics to a local file using the **performance-mgmt resources dump local** command.
- You can filter performance management instances by defining a regular expression group (**performance-mgmt regular-expression** command), which includes multiple regular expression indices that specify strings to match. You apply a defined regular expression group to one or more statistics or threshold templates in the **performance-mgmt statistics interface** or **performance-mgmt thresholds interface** commands.

## Frequency Synchronization and SyncE

Cisco IOS XR Software supports SyncE-capable Ethernet on the router. Frequency Synchronization enables you to distribute the precision clock signals around the network. The system injects a highly accurate timing signal into the router in the network. The timing signals use an external timing technology, such as Cesium atomic clocks, or GPS, and then pass the signals to the physical interfaces of the router. Peer routers can then recover this precision frequency from the line, and also transfer it around the network. This feature is traditionally applicable to SONET or SDH networks, but is now available on Ethernet for Cisco 8000 Series Router with Synchronous Ethernet capability. For more information, see *Cisco 8000 Series Router System Management Configuration Guide*.

## LLDP

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the Data Link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches). CDP allows network management applications to automatically discover and learn about other Cisco devices connected to the network.

To support non-Cisco devices and to allow for interoperability between other devices, the router also supports the IEEE 802.1AB Link Layer Discovery Protocol (LLDP). LLDP is also a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the Data Link Layer, which allows two systems running different network layer protocols to learn about each other.

LLDP supports a set of attributes that it uses to learn information about neighbor devices. These attributes have a defined format known as a Type-Length-Value (TLV). LLDP supported devices can use TLVs to receive and send information to their neighbors. Details such as configuration information, device capabilities, and device identity can be advertised using this protocol.

In addition to the mandatory TLVs (Chassis ID, Port ID, End of LLDPDU, and Time-to-Live), the router also supports the following basic management TLVs, which are optional:

- Port Description
- System Name
- System Description
- System Capabilities
- Management Address

These optional TLVs are automatically sent when LLDP is active, but you can disable them as needed using the **lldp tlv-select <Optional TLV> disable** command.




---

**Note** For LLDP to work on any bundle member, enable LLDP on the bundle main interface either globally or on the interface itself. You can then choose to disable LLDP transmission on bundle main interface by using the `lldp transmit disable` command.

You can also control LLDP transmit or receive on each bundle member interface as desired.

---

## LLDP Frame Format

LLDP frames use the IEEE 802.3 format, which consists of the following fields:

- Destination address (6 bytes)—Uses a multicast address of 01-80-C2-00-00-0E.
- Source address (6 bytes)—MAC address of the sending device or port.
- LLDP Ethertype (2 bytes)—Uses 88-CC.
- LLDP PDU (1500 bytes)—LLDP payload consisting of TLVs.
- FCS (4 bytes)—Cyclic Redundancy Check (CRC) for error checking.

## LLDP TLV Format

LLDP TLVs carry the information about neighboring devices within the LLDP PDU using the following basic format:

- TLV Header (16 bits), which includes the following fields:
  - TLV Type (7 bits)
  - TLV Information String Length (9 bits)
- TLV Information String (0 to 511 bytes)

## Specifying User-Defined LLDP TLV Values

It is possible to override the system default values for some of the mandatory LLDP Type-Length-Values (TLVs) that are advertised by routers to their directly connected neighboring devices. While advertising their identity and capabilities, routers can assign user-defined meaningful names instead of autogenerated values. Using the following CLIs you can specify these user-defined values:

- Router(config)#lldp system-name *system-name*
- Router(config)#lldp system-description *system-description*
- Router(config)#lldp chassis-id-type *chassis-type*
- Router(config)#lldp chassis-id *local-chassis-id*



**Note** The **chassis-id** value is configurable only when the **chassis-id-type** is set as **Local**. If there is a mismatch, you encounter a configuration failed error message.

The configured values, such as the system name, system description, chassis-id, chassis-type become part of the TLV in the LLDP packets that are sent to its neighbors. Values are transmitted only to LLDP enabled interfaces to which the router is connected.

You can assign any of the following values for the `chassis-id-type`. The chassis-id-types are objects that are part of the [management information base \(MIB\)](#). Depending on the selected chassis-id-type, values are assigned to these objects, and they are advertised by the router to its neighboring devices.

chassis-id-type	Description
chassis-component	Chassis identifier based on the value of entPhysicalAlias object that is defined in IETF RFC 2737.
interface-alias	Chassis identifier based on the value of ifAlias object as defined in IETF RFC 2863.
interface-name	Chassis identifier based on the name of the interface.
local	Chassis identifier based on a locally defined value.
mac-address	Chassis identifier based on the value of a unicast source address.
network-address	Chassis identifier based on a network address that is associated with a particular chassis.
port-component	Chassis identifier based on the value of entPhysicalAlias object defined in IETF RFC 2737 for a port or backplane component.



**Tip** You can programmatically modify default values of LLDP TLVs by using the `openconfig-lldp` OpenConfig data model. To get started with using data models, see the *Programmability Configuration Guide for Cisco 8000 Series Routers*.

### Configuration Example

This example shows the configuration for the LLDP TLVs that will be advertised by routers to their directly connected neighboring devices.

```
Router(config)#lldp system-name cisco-xr
Router(config)#lldp system-description cisco-xr-edge-device
Router(config)#lldp chassis-id-type local
Router(config)#lldp chassis-id ce-device9
```

### Running Configuration

```
Router#show lldp
Tue Sep 13 16:03:44.550 +0530
Global LLDP information:
Status: ACTIVE
LLDP Chassis ID: ce-device9
LLDP Chassis ID Subtype: Locally Assigned Chassis Subtype
LLDP System Name: cisco-xr
LLDP advertisements are sent every 30 seconds
LLDP hold time advertised is 120 seconds
LLDP interface reinitialisation delay is 2 seconds
```

## LLDP Operation

LLDP is a one-way protocol. The basic operation of LLDP consists of a device enabled for transmit of LLDP information sending periodic advertisements of information in LLDP frames to a receiving device.

Devices are identified using a combination of the Chassis ID and Port ID TLVs to create an MSAP (MAC Service Access Point). The receiving device saves the information about a neighbor in a remote lldp cache for a certain amount of time as specified in the TTL TLV received from the neighbor, before aging and removing the information.

LLDP supports the following additional operational characteristics:

- LLDP can operate independently in transmit or receive modes. On global lldp enablement, the default mode is to operate in both transmit and receive modes.
- LLDP operates as a slow protocol with transmission speeds not greater than one frame per five seconds.
- LLDP packets are sent when the following occurs:
  - The packet update frequency specified by the **lldp timer** command is reached. The default is 30 seconds.
  - When a change in the values of the managed objects occurs from the local system's LLDP MIB.
  - When LLDP is activated on an interface (3 frames are sent upon activation similar to CDP).
- When an LLDP frame is received, the LLDP remote services and PTOPO MIBs are updated with the information in the TLVs.



- LLDP supports the following actions on these TLV characteristics:
  - Interprets a neighbor TTL value of 0 as a request to automatically purge the information of the transmitting device. These shutdown LLDPDUs are typically sent prior to a port becoming inoperable.
  - An LLDP frame with a malformed mandatory TLV is dropped.
  - A TLV with an invalid value is ignored.
  - A copy of an unknown organizationally-specific TLV is maintained if the TTL is non-zero, for later access through network management.

## Supported LLDP Functions

The router supports the following LLDP functions:

- IPv4 and IPv6 management addresses—In general, both IPv4 and IPv6 addresses will be advertised if they are available, and preference is given to the address that is configured on the transmitting interface. If the transmitting interface does not have a configured address, then the system populates the TLV with an address from another interface. The advertised LLDP IP address is implemented according to the following priority order of IP addresses for interfaces on the router:
  - Locally configured address on the transmitting interface
  - MgmtEth0/RSP0RP0/CPU0/0
  - MgmtEth0/RSP0RP0/CPU0/1
  - MgmtEth0/RSP1RP1/CPU0/0
  - MgmtEth0/RSP1RP1/CPU0/1
  - Loopback interfaces

There are some differences between IPv4 and IPv6 address management in LLDP:

- For IPv4, as long as the IPv4 address is configured on an interface, it can be used as an LLDP management address.
- For IPv6, after the IPv6 address is configured on an interface, the interface status must be Up and pass the DAD (Duplicate Address Detection) process before it can be used as an LLDP management address.
- LLDP is supported for the nearest physically attached, non-tunneled neighbors.
- LLDP is supported for Ethernet interfaces, L3 subinterfaces, bundle interfaces, and L3 bundle subinterfaces.

## Unsupported LLDP Functions

The following LLDP functions are not supported on the router:

- LLDP-MED organizationally unique extension—However, interoperability still exists between other devices that do support this extension.
- Tunneled neighbors, or neighbors more than one hop away.

- LLDP TLVs cannot be disabled on a per-interface basis; However, certain optional TLVs can be disabled globally.
- LLDP SNMP trap `lldpRemTablesChange`.

## Setting the Carrier Delay on Physical Interfaces

Table 10: Feature History Table

Feature Name	Release Information	Feature Description
Setting the Carrier Delay on Physical Interfaces	Release 7.5.4	<p>You can configure the Ethernet interfaces to delay the processing of hardware link-down and link-up notifications. With this functionality, the interface state remains stable for the configured delay duration, even if the hardware link state fluctuates. This prevents interface flapping and improves network reliability.</p> <p>Use the following CLI command in interface configuration mode to configure the delay time:</p> <p><b>carrier-delay</b></p>

Hardware links may take time to stabilize after a state change and may experience link flaps. Link flap is a situation in which a physical interface on the router continually goes up and down in a brief period of time. Administrators may not want to bring up or take down ports when flaps happen in short period to avoid network re-convergence.

To ensure that hardware link state is stable before an action is taken on the interface, the carrier-delay functionality introduces a delay in bringing up the Ethernet interface after a link state change. This delay can be configured to provide sufficient time for the hardware link state to stabilize.

When there is a change in the link state, the carrier-delay timer starts. If the link state goes up, the **carrier-delay up** timer starts. During this delay period, the Ethernet interface state remains down even if the link is physically restored. Set a delay duration that ensures a stable link state is established before the interface becomes operational again. This delay helps to avoid unnecessary interface state changes and associated traffic rerouting.

Similarly, when the link state comes down, the **carrier-delay down** timer starts. When you delay the processing of hardware link-down notifications, the higher layer routing protocols are unaware of the link state. During this delay period, the Ethernet interface remains up even though the hardware link is down. This delay allows the line protection equipment to intervene and possibly bring back up the physical link. If such an intervention happens and the link goes up within the timer expiry, the interface state remains up. Otherwise, after the timer expiry, the interface state goes down.

**Note**

- If the **carrier-delay down** *milliseconds* command is configured on a physical link that fails and cannot be recovered, link down detection time increases, and it may take longer for the routing protocols to reroute the traffic around the failed link.
- Carrier-delay is not configured by default. If carrier-delay is not configured, the higher layer protocols are notified as quickly as possible when a physical link state changes.
- You can configure carrier-delay for only link-up, only link-down, or both link-up and link-down notifications.

**Configuration Example**

In this example, both link-up and link-down notifications are configured to be delayed by 100 ms using **carrier-delay** command.

```
Router#configure
Router(config)#interface HundredGigE 0/0/0/0
Router(config-if)#carrier-delay up 200 down 200
```

**Running Configuration**

```
interface HundredGigE0/0/0/0
carrier-delay up 100 down 100
!
```

**Verification**

Enter the **show interfaces** command to see the current state of the carrier-delay configuration for an interface.

```
Router#show interfaces HundredGigE 0/0/0/0 | include Carrier
Fri Mar 31 07:25:05.273 UTC
Carrier delay (up) is 100 msec, Carrier delay (down) is 100 msec
Router#
```

## How to Configure Ethernet

This section provides the following configuration procedures:

### Configuring LLDP



**Note** LLDP is not supported on the FP-X line cards.

This section includes the following configuration topics for LLDP:

## LLDP Default Configuration

This table shows the values of the LLDP default configuration on the router. To change the default settings, use the LLDP global configuration and LLDP interface configuration commands.

LLDP Function	Default
LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	2 seconds
LLDP TLV selection	All TLVs are enabled for sending and receiving.
LLDP interface state	Enabled for both transmit and receive operation when LLDP is globally enabled.

## Enabling LLDP Per Interface

When you enable LLDP globally, all interfaces that support LLDP are automatically enabled for both transmit and receive operations. However, if you want to enable LLDP per interface, perform the following configuration steps:

```
RP/0/RSP0/CPU0:ios(config)# int HundredGigE 0/2/0/0
RP/0/RSP0/CPU0:ios(config-if)# no sh
RP/0/RSP0/CPU0:ios(config-if)#commit
RP/0/RSP0/CPU0:ios(config-if)#lldp ?
RP/0/RSP0/CPU0:ios(config-if)#lldp enable
RP/0/RSP0/CPU0:ios(config-if)#commit
```

### Running configuration

```
RP/0/RSP0/CPU0:ios#sh running-config
Wed Jun 27 12:40:21.274 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Wed Jun 27 00:59:29 2018 by UNKNOWN
!
interface HundredGigE0/1/0/0
 shutdown
!
interface HundredGigE0/1/0/1
 shutdown
!
interface HundredGigE0/1/0/2
 shutdown
!
interface HundredGigE0/2/0/0
 Shutdown
!
interface HundredGigE0/2/0/1
 shutdown
!
interface HundredGigE0/2/0/2
 shutdown
!
end
```

## Verification

```

Verifying the config
=====
RP/0/RSP0/CPU0:ios#sh lldp interface <===== LLDP enabled only on GigEth0/2/0/0
Wed Jun 27 12:43:26.252 IST

HundredGigE0/2/0/0:
  Tx: enabled
  Rx: enabled
  Tx state: IDLE
  Rx state: WAIT FOR FRAME
RP/0/RSP0/CPU0:ios#

RP/0/RSP0/CPU0:ios# show lldp neighbors
Wed Jun 27 12:44:38.977 IST
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID      Local Intf      Hold-time  Capability  Port ID
ios            Gi0/2/0/0      120        R           Gi0/2/0/0      <===== LLDP
enabled only on GigEth0/2/0/0 and neighborhood seen for the same.

Total entries displayed: 1

RP/0/RSP0/CPU0:ios#

```

## Enabling LLDP Globally

To run LLDP on the router, you must enable it globally. When you enable LLDP globally, all interfaces that support LLDP are automatically enabled for both transmit and receive operations.

You can override this default operation at the interface to disable receive or transmit operations. For more information about how to selectively disable LLDP receive or transmit operations for an interface, see the *Disabling LLDP Receive and Transmit Operation for an Interface* section.



**Note** For LLDP to work on any bundle member, enable LLDP on the bundle main interface either globally or on the interface itself. You can then choose to disable LLDP transmission on bundle main interface by using the `lldp transmit disable` command.

You can also control LLDP transmit or receive on each bundle member interface as desired.

The following table describes the global attributes that you can configure:

Attribute	Default	Range	Description
Holdtime	120	0-65535	Specifies the holdtime (in sec) that are sent in packets
Reinit	2	2-5	Delay (in sec) for LLDP initialization on any interface

Attribute	Default	Range	Description
Timer	30	5-65534	Specifies the rate at which LLDP packets are sent (in sec)

To enable LLDP globally, complete the following steps:

1. RP/0//CPU0:router # configure
2. RP/0//CPU0:router(config) #lldp
3. end or commit

### Running configuration

```
RP/0/RP0/CPU0:turin-5#show run lldp
Fri Dec 15 20:36:49.132 UTC
lldp
!
```

```
RP/0/RP0/CPU0:turin-5#show lldp neighbors
Fri Dec 15 20:29:53.763 UTC
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

```
Device ID          Local Intf          Hold-time  Capability  Port ID
SW-NOSTG-I11-PUB.cis Mg0/RP0/CPU0/0    120        N/A         Fa0/28
```

Total entries displayed: 1

```
RP/0/RP0/CPU0:turin-5#show lldp neighbors mgmtEth 0/RP0/CPU0/0
Fri Dec 15 20:30:54.736 UTC
Capability codes:
```

```
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

```
Device ID          Local Intf          Hold-time  Capability  Port ID
SW-NOSTG-I11-PUB.cis Mg0/RP0/CPU0/0    120        N/A         Fa0/28
```

Total entries displayed: 1

## Configuring Global LLDP Operational Characteristics

When you enable LLDP globally on the router using the **lldp** command, these defaults are used for the protocol.

To modify the global LLDP operational characteristics such as the LLDP neighbor information holdtime, initialization delay, or packet rate, complete the following steps:

### Step 1 Example:

```
/CPU0:router# configure
```

Enters global configuration mode.

### Step 2 **lldp holdtime** *seconds*

**Example:**

```
RP/0//CPU0:router(config)#lldp holdtime 60
```

(Optional) Specifies the length of time that information from an LLDP packet should be held by the receiving device before aging and removing it.

**Step 3** **lldp reinit** *seconds*

**Example:**

```
RP/0//CPU0:router(config)# lldp reinit 4
```

(Optional) Specifies the length of time to delay initialization of LLDP on an interface.

**Step 4** **lldp timer** *seconds*

**Example:**

```
RP/0//CPU0:router(config)#lldp reinit 60
```

(Optional) Specifies the LLDP packet rate.

**Step 5** **end** or **commit**

**Example:**

```
RP/0//CPU0:router(config)# end
```

or

```
RP/0//CPU0:router(config)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?  
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

---

## Disabling Transmission of Optional LLDP TLVs

Certain TLVs are classified as mandatory in LLDP packets, such as the Chassis ID, Port ID, and Time to Live (TTL) TLVs. These TLVs must be present in every LLDP packet. You can suppress transmission of certain other optional TLVs in LLDP packets.

To disable transmission of optional LLDP TLVs, complete the following steps:

### Step 1 **configure**

#### Example:

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

Enters global configuration mode.

### Step 2 **lldp tlv-select tlv-name disable**

#### Example:

```
RP/0/RSP0/CPU0:router(config)# lldp tlv-select system-capabilities disable
```

(Optional) Specifies that transmission of the selected TLV in LLDP packets is disabled. The *tlv-name* can be one of the following LLDP TLV types:

- **management-address**
- **port-description**
- **system-capabilities**
- **system-description**
- **system-name**

### Step 3 **end** or **commit**

#### Example:

```
RP/0/RSP0/CPU0:router(config)# end
```

or

```
RP/0/RSP0RP0/CPU0:router(config)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?  
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.



- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

---

## Disabling LLDP Receive and Transmit Operation for an Interface

When you enable LLDP globally on the router, all supported interfaces are automatically enabled for LLDP receive and transmit operation. You can override this default by disabling these operations for a particular interface.

To disable LLDP receive and transmit operations for an interface, complete the following steps:

---

### Step 1 **configure**

**Example:**

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

Enters global configuration mode.

### Step 2 **interface HundredGigE 0/2/0/0**

**Example:**

```
RP/0/RSP0RCP0/CPU0:router (config) #interface HundredGigE 0/2/0/0
```

Enters interface configuration mode and specifies the Ethernet interface name and notation *rack/slot/module/port*. Possible interface types for this procedure are:

- HundredGigE
- TenGigE

### Step 3 **lldp**

**Example:**

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

(Optional) Enters LLDP configuration mode for the specified interface.

### Step 4 **receive disable**

**Example:**

```
RP/0/RSP0/CPU0:router (config-lldp) #receive disable
```

(Optional) Disables LLDP receive operations on the interface.

### Step 5 **transmit disable**

**Example:**

```
RP/0/RSP0/CPU0:router (config-lldp) #transmit disable
```

(Optional) Disables LLDP transmit operations on the interface.

**Step 6** **end** or **commit****Example:**

```
RP/0/RSP0/CPU0:router(config)# end
```

or

```
RP/0/RSP0/CPU0:router(config)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

## Verifying the LLDP Configuration

This section describes how you can verify the LLDP configuration both globally and for a particular interface.

### Verifying the LLDP Global Configuration

To verify the LLDP global configuration status and operational characteristics, use the **show lldp** command as shown in the following example:

```
RP/0/RSP0/CPU0:router# show lldp
Wed Apr 13 06:16:45.510 DST
Global LLDP information:
  Status: ACTIVE
  LLDP advertisements are sent every 30 seconds
  LLDP hold time advertised is 120 seconds
  LLDP interface reinitialisation delay is 2 seconds
```

If LLDP is not enabled globally, the following output appears when you run the **show lldp** command:

```
RP/0/RSP0/CPU0:router# show lldp
Wed Apr 13 06:42:48.221 DST
% LLDP is not enabled
```

## Verifying the LLDP Interface Configuration

To verify the LLDP interface status and configuration, use the **show lldp interface** command as shown in the following example:

```
RP/0/RSP0/CPU0:router# show lldp interface HundredGigE 0/1/0/7
Wed Apr 13 13:22:30.501 DST

HundredGigE0/1/0/7:
  Tx: enabled
  Rx: enabled
  Tx state: IDLE
  Rx state: WAIT FOR FRAME
```

To monitor and maintain LLDP on the system or get information about LLDP neighbors, use one of the following commands:

Command	Description
<b>clear lldp counters</b>	Resets LLDP traffic counters or LLDP neighbor information.
<b>show lldp entry</b>	Displays detailed information about LLDP neighbors.
<b>show lldp errors</b>	Displays LLDP error and overflow statistics.
<b>show lldp neighbors</b>	Displays information about LLDP neighbors.
<b>show lldp traffic</b>	Displays statistics for LLDP traffic.

To collect or clear LLDP interface statistics, you can use the following commands:

Command	Description
<b>show lldp traffic interface</b> <i>interface_name</i>	Displays LLDP traffic statistics for the specified interface.
<b>clear lldp counters interface</b> <i>interface_name</i>	Clears LLDP traffic statistics for the specified interface. Global statistics remains intact. Similarly, clearing global statistics does not impact the interface statistics.

### Examples for LLDP Interface Statistics

This example shows interface statistics for **gigabitEthernet0/0/0/0**:

```
Router#show lldp traffic interface gigabitEthernet0/0/0/0
```

This example clears the interface statistics for **gigabitEthernet0/0/0/0**.

```
Router#show lldp traffic interface gigabitEthernet0/0/0/0
```

### Running Configuration

```
Router#show lldp traffic interface gigabitEthernet 0/2/0/8
Wed Aug 24 17:38:11.829 IST
```

```
LLDP Interface statistics:
```

```

Total frames out: 28786
Total frames in: 38417
Total frames received in error: 0
Total frames out error: 0
Total frames discarded: 0
Total TLVs discarded: 0
Total TLVs unrecognized: 0

```

## Configuration Examples for Ethernet

This section provides the following configuration examples:

### Configuring an Ethernet Interface: Example

The following example shows how to configure an interface for a 10-Gigabit Ethernet modular services card:

```

RP/0//CPU0:router# configure
RP/0//CPU0:router(config)# interface TenGigE 0/0/0/1
RP/0//CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224
RP/0//CPU0:router(config-if)# flow-control ingress
RP/0//CPU0:router(config-if)# mtu 1448
RP/0//CPU0:router(config-if)# mac-address 0001.2468.ABCD
RP/0//CPU0:router(config-if)# no shutdown
RP/0//CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes

```

```

RP/0//CPU0:router# show interfaces TenGigE 0/0/0/1

TenGigE0/0/0/1 is down, line protocol is down
  Hardware is TenGigE, address is 0001.2468.abcd (bia 0001.81a1.6b23)
  Internet address is 172.18.189.38/27
  MTU 1448 bytes, BW 10000000 Kbit
    reliability 0/255, txload Unknown, rxload Unknown
  Encapsulation ARPA,
    Full-duplex, 10000Mb/s, LR
    output flow control is on, input flow control is on
  Encapsulation ARPA,
  ARP type ARPA, ARP timeout 01:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
  Received 0 broadcast packets, 0 multicast packets
    0 runts, 0 giants, 0 throttles, 0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets
  0 output errors, 0 underruns, 0 applique, 0 resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions

```

### Configuring LLDP: Examples

The following example shows how to enable LLDP globally on the router and modify the default LLDP operational characteristics:

```
RP/0//CPU0:router# configure
RP/0//CPU0:router(config)# lldp
RP/0//CPU0:router(config)# lldp holdtime 60
RP/0//CPU0:router(config)# lldp reinit 4
RP/0//CPU0:router(config)# lldp timer 60
RP/0//CPU0:router(config)# commit
```

The following example shows how to disable a specific Gigabit Ethernet interface for LLDP transmission:

```
RP/0//CPU0:router# configure
RP/0//CPU0:router(config)# interface HundredGigE 0/2/0/0
RP/0//CPU0:router(config-if)# lldp
RP/0//CPU0:router(config-lldp)# transmit disable
```

### Where to Go Next

When you have configured an Ethernet interface, you can configure individual VLAN subinterfaces on that Ethernet interface.

For information about modifying Ethernet management interfaces for the shelf controller (SC), route processor (RP), and distributed RP, see the Advanced Configuration and Modification of the Management Ethernet Interface later in this document.

For information about IPv6 see the Implementing Access Lists and Prefix Lists on Cisco IOS XR Software module in the Cisco IOS XR IP Addresses and Services Configuration Guide.

## Configuring a Layer 2 VPN AC: Example

The following example indicates how to configure a Layer 2 VPN AC on an Ethernet interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/0/0/2
RP/0/RSP0/CPU0:router(config-if)# l2transport
RP/0/RSP0/CPU0:router(config-if-l2)# l2protocol tunnel
RP/0/RSP0/CPU0:router(config-if-l2)# commit
```

## Configuring Physical Ethernet Interfaces

Use this procedure to create a basic Ethernet interface configuration.

### Step 1 **show version**

#### Example:

```
RP/0/RP0/CPU0:router# show version
```

(Optional) Displays the current software version, and can also be used to confirm that the router recognizes the line card.

### Step 2 **show interfaces [ TenGigE FortyGigE HundredGigE FourHundredGigE ] interface-path-id**

#### Example:

```
RP/0/RP0/CPU0:router# show interface HundredGigE 0/1/0/1
```

(Optional) Displays the configured interface and checks the status of each interface port.

**Step 3** **configure**

**Example:**

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

Enters global configuration mode.

**Step 4** **show interfaces [ TenGigE FortyGigE HundredGigE FourHundredGigE] interface-path-id**

**Example:**

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/1/0/1
```

Enters interface configuration mode and specifies the Ethernet interface name and notation *rack/slot/module/port*. Possible interface types for this procedure are:

- 10GigE
- 40GigE
- 100GigE

**Note** • The example indicates a 100-Gigabit Ethernet interface in the line card in slot 1.

- 400GigE

The examples of *interface-path-id* ranges are:

- **TenGigE** — 0/0/0/0 - 0/0/0/31
- **FortyGigE** — 0/0/1/0 - 0/0/1/1
- **HundredGigE** — 0/0/1/0 - 0/0/1/1

**Step 5** **ipv4 address ip-address mask**

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224
```

Assigns an IP address and subnet mask to the interface.

- Replace *ip-address* with the primary IPv4 address for the interface.
- Replace *mask* with the mask for the associated IP subnet. The network mask can be specified in either of two ways:
  - The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means that the corresponding address bit belongs to the network address.
  - The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address.

**Step 6** **flow-control {bidirectional| egress | ingress}**

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# flow control ingress
```

(Optional) Enables the sending and processing of flow control pause frames.

- **egress**—Enables the sending of flow control pause frames in egress.
- **ingress**—Enables the processing of received pause frames on ingress.
- **bidirectional**—Enables the sending of flow control pause frames in egress and the processing of received pause frames on ingress.

**Step 7**     **mtu bytes****Example:**

```
RP/0/RP0/CPU0:router(config-if)# mtu 1448
```

(Optional) Sets the MTU value for the interface.

- The default is 1514 bytes for normal frames and 1518 bytes for 802.1Q tagged frames.
- The range for 100-Gigabit Ethernet mtu values is 64 bytes to 65535 bytes.

**Step 8**     **no shutdown****Example:**

```
RP/0/RP0/CPU0:router(config-if)# no shutdown
```

Removes the shutdown configuration, which forces an interface administratively down.

**Step 9**     **end or commit****Example:**

```
RP/0/RP0/CPU0:router(config-if)# end
```

or

```
RP/0/RP0/CPU0:router(config-if)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?  
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

**Step 10** `show interfaces [ TenGigE FortyGigE HundredGigE FourHundredGigE ] interface-path-id`

**Example:**

```
RP/0/RP0/CPU0:router# show interfaces HundredGigE 0/1/0/1
```

(Optional) Displays statistics for interfaces on the router.

**Example**

This example shows how to configure an interface for a 100-Gigabit Ethernet line card:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224

RP/0/RP0/CPU0:router(config-if)# mtu 1448

RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes
```

```
RP/0/RP0/CPU0:router# show interfaces HundredGigE 0/5/0/24
HundredGigE0/5/0/24 is up, line protocol is up
  Interface state transitions: 1
  Hardware is HundredGigE, address is 6219.8864.e330 (bia 6219.8864.e330)
  Internet address is 3.24.1.1/24
  MTU 9216 bytes, BW 100000000 Kbit (Max: 100000000 Kbit)
    reliability 255/255, txload 3/255, rxload 3/255
  Encapsulation ARPA,
  Full-duplex, 100000Mb/s, link type is force-up
  output flow control is off, input flow control is off
  Carrier delay (up) is 10 msec
  loopback not set,
  Last link flapped 10:05:07
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:08:56, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 1258567000 bits/sec, 1484160 packets/sec
  5 minute output rate 1258584000 bits/sec, 1484160 packets/sec
    228290765840 packets input, 27293508436038 bytes, 0 total input drops
      0 drops for unrecognized upper-level protocol
    Received 15 broadcast packets, 45 multicast packets
      0 runts, 0 giants, 0 throttles, 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  212467849449 packets output, 25733664696650 bytes, 0 total output drops
  Output 23 broadcast packets, 15732 multicast packets
  39 output errors, 0 underruns, 0 applique, 0 resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
```



```
RP/0/RP0/CPU0:router# show running-config interface HundredGigE 0/5/0/24

interface HundredGigE 0/5/0/24
  mtu 9216
  service-policy input linerate
  service-policy output elinerate
  ipv4 address 3.24.1.1 255.255.255.0
  ipv6 address 3:24:1::1/64
  flow ipv4 monitor perfv4 sampler fsm ingress
!
```

## Viewing Interface Counters Report

The Interface Counters report summarizes the statistics for all interfaces configured on the router.

The report displays the interfaces configured, the input and output rate, the total number of packets transmitted and received, the time interval, the current status of each interface, and the packet counts for input and output broadcast, multicast, and errored packets.

The **show interfaces** command, displays statistics per interface with many lines of data. The traffic rate displays the average number of packets received per second over the load interval. The load interval is configurable on the physical and bundle main interface. The report displays the load on the interface for a longer duration of time and does not show a spike in the traffic rate. This rate is the exponentially weighted average with a time constant of the load interval.



---

**Note** For the average to be within two percent of the instantaneous rate of a uniform stream of traffic, four times the load interval must pass.

---

For more information about the use of **show interfaces** command, see *Interface and Hardware Component Command Reference for Cisco 8000 Series Routers*.

## Instant Display of Traffic Rates for all the Physical Interfaces

Table 11: Feature History Table

Feature Name	Release Information	Feature Description
Instant display of traffic rates on all physical interfaces	Release 7.5.4	<p>You can now display a snapshot of the traffic throughput and traffic rate on all physical interfaces over the last few seconds. We have introduced a <b>show</b> command to view the counters and rate information for the interfaces.</p> <p>The feature introduces these:</p> <ul style="list-style-type: none"> <li>• CLI: <b>show interfaces counter rates physical</b></li> <li>• YANG Data Model: <b>Cisco-IOS-XR-infra-statsd-oper:yang</b> (see <a href="#">GitHub</a> under the 754 folder.)</li> </ul>

The new **show** command displays a snapshot of statistics for all the interfaces at a given instant for your quick reference. Here, the display is in a tabular format for easy analysis.

Run the **show interfaces counter rates physical** command to view statistics of all physical interfaces.

### View the statistics

```
Router#show interfaces counters rates physical
```

```

InterfaceName      Intvl  InMbps  InBW%  InKpps  OutMbps  OutBW%  OutKpps
GigabitEthernet0/2/0/0  0:05   0.0     0.0%   0.0     0.0     0.0%   0.0
GigabitEthernet0/2/0/1  0:05   0.0     0.0%   0.0     0.0     0.0%   0.0
GigabitEthernet0/2/0/2  0:05   0.0     0.0%   0.0     0.0     0.0%   0.0
GigabitEthernet0/2/0/3  0:05  235.0   22.0%  23.5    87.0     9.5%   7.2
GigabitEthernet0/3/0/0  0:05   88.0    9.3%   7.0    100.0    10.0%  10.5
GigabitEthernet0/3/0/1  0:05   0.0     0.0%   0.0     0.0     0.0%   0.0

```

The statistics for each physical interface is calculated for the time interval of 5 sec. Hence, the input and output rate (in Mbps and Kpps) is the real-time statistics.



**Note** The traffic rate displayed is the real-time link utilization of the time interval. The time interval is determined by the system and may vary based on the system processing load. The time interval increases during events where the system is handling, for example, performing routing updates.

# How to Configure Interfaces in Breakout Mode

## Information About Breakout

The router supports transmission of traffic in the breakout mode. The breakout mode enables a 40 Gigabit Ethernet port to be split into four independent and logical 10 Gigabit Ethernet ports. The 4x10 breakout mode is supported on the following types of 40G modules:

- QSFP-4x10-LR-S
- QSFP-40G-SR4

### Guidelines and Restrictions for Breakout Mode

- The native 40G mode on QSFP-40G-SR4 is not supported.
- The 36-port QSFP56-DD 400 GbE Line Card does not support the 4x10G breakout.
- If you're using a Q100-based Cisco 8200 Series Router and want to set up a 4x10G breakout configuration, you need to use even numbered ports from 24 to 35. These include ports 24, 26, 28, 30, 32, and 34. Once you do this, the system automatically disables the odd numbered ports in this range - ports 25, 27, 29, 31, 33, and 35.
- Use the *hw-module port-range* command to set the port range for the breakout configuration in the global configuration.
- To remove the global *hw-module port-range* configuration, you must first remove the 'breakout 4x10' configuration under the controller.
- For 4x10G breakout on 48-port Line Card, only QSFP-4x10-LR-S module is supported.

## Configure Breakout in a Port

Configuring breakout in a port:

```
RP/0/RP0/CPU0:uut# configure
Fri Oct 11 23:58:47.165 UTC
RP/0/RP0/CPU0:uut(config)# controller optics 0/1/0/28
RP/0/RP0/CPU0:uut(config-Optics)# breakout 4x10
RP/0/RP0/CPU0:uut(config-Optics)# commit
Fri Oct 11 23:59:51.261 UTC
RP/0/RP0/CPU0:uut(config-Optics)# end
RP/0/RP0/CPU0:uut#
```

## Remove the Breakout Configuration

Removing the breakout configuration:

```
RP/0/RP0/CPU0:uut# configure
Sat Oct 12 00:01:38.673 UTC
RP/0/RP0/CPU0:uut(config)# controller optics 0/1/0/28
RP/0/RP0/CPU0:uut(config-Optics)# no breakout 4x10
RP/0/RP0/CPU0:uut(config-Optics)# commit
```

```
Sat Oct 12 00:01:55.864 UTC
RP/0/RP0/CPU0:ut(config-Optics)# end
```

## Verify a Breakout Configuration

Verifying a breakout configuration:

```
RP/0/RP0/CPU0:ut# show running-config controller optics 0/1/0/28
Sat Oct 12 00:11:33.962 UTC
controller Optics0/1/0/28
breakout 4x10
!
```

```
RP/0/RP0/CPU0:ut# show int br location 0/1/CPU0 | i Te
Sat Oct 12 00:11:38.609 UTC
      Te0/1/0/27/0      up          up          ARPA 10000    10000000
      Te0/1/0/27/1      up          up          ARPA 10000    10000000
      Te0/1/0/27/2      up          up          ARPA 10000    10000000
      Te0/1/0/27/3      up          up          ARPA 10000    10000000
      Te0/1/0/28/0      up          up          ARPA 10000    10000000
      Te0/1/0/28/1      up          up          ARPA 10000    10000000
      Te0/1/0/28/2      up          up          ARPA 10000    10000000
      Te0/1/0/28/3      up          up          ARPA 10000    10000000
```



## CHAPTER 5

# Configuring Ethernet OAM

This module describes the configuration of Ethernet Operations, Administration, and Maintenance (OAM):

**Table 12: Feature Information Table**

Release	Modification
Release 7.3.1	Support for Ethernet Link OAM was introduced.

- [Information About Configuring Ethernet OAM, on page 55](#)
- [Configuring Ethernet OAM, on page 58](#)
- [Configuration Examples for Ethernet OAM, on page 66](#)
- [Ethernet CFM, on page 69](#)
- [How to Configure Ethernet OAM, on page 81](#)
- [CFM Over Bundles, on page 103](#)
- [Ethernet Frame Delay Measurement for L2VPN Services, on page 104](#)

## Information About Configuring Ethernet OAM

To configure Ethernet OAM, you should understand the following concepts:

## Ethernet Link OAM

Table 13: Feature History Table

Feature Name	Release Information	Feature Description
Ethernet Link OAM	Release 7.3.1	This feature allow Service Providers to monitor the quality of the connections on a MAN or WAN. Service providers can monitor specific events, and take actions on events. Ethernet link OAM operates on a single, physical link and it can be configured to monitor either side or both sides of that link.

Ethernet as a Metro Area Network (MAN) or a Wide Area Network (WAN) technology benefits greatly from the implementation of Operations, Administration and Maintenance (OAM) features. Ethernet link OAM features allow Service Providers to monitor the quality of the connections on a MAN or WAN. Service providers can monitor specific events, and take actions on events. Ethernet link OAM operates on a single, physical link and it can be configured to monitor either side or both sides of that link.

Ethernet link OAM can be configured in the following ways:

- A Link OAM profile can be configured, and this profile can be used to set the parameters for multiple interfaces.
- Link OAM can be configured directly on an interface.

When an interface is also using a link OAM profile, specific parameters that are set in the profile can be overridden by configuring a different value directly on the interface.

An Ethernet Link OAM profile simplifies the process of configuring EOAM features on multiple interfaces. An Ethernet OAM profile, and all of its features, can be referenced by other interfaces, allowing other interfaces to inherit the features of that Ethernet OAM profile.

Individual Ethernet link OAM features can be configured on individual interfaces without being part of a profile. In these cases, the individually configured features always override the features in the profile.

The preferred method of configuring custom EOAM settings is to create an EOAM profile in Ethernet configuration mode and then attach it to an individual interface or to multiple interfaces.

These standard Ethernet Link OAM features are supported on the router:

## Neighbor Discovery

Neighbor discovery enables each end of a link to learn the OAM capabilities of the other end and establish an OAM peer relationship. Each end also can require that the peer have certain capabilities before it will establish a session. You can configure certain actions to be taken if there is a capabilities conflict or if a discovery process times out, using the **action capabilities-conflict** or **action discovery-timeout** commands.

## EFD

Ethernet Fault Detection (EFD) is a mechanism that allows Ethernet OAM protocols to control the line protocol state of an interface.

Unlike many other interface types, Ethernet interfaces do not have a line protocol, whose state is independent from that of the interface. For Ethernet interfaces, this role is handled by the physical-layer Ethernet protocol itself, and therefore if the interface is physically up, then it is available and traffic can flow.

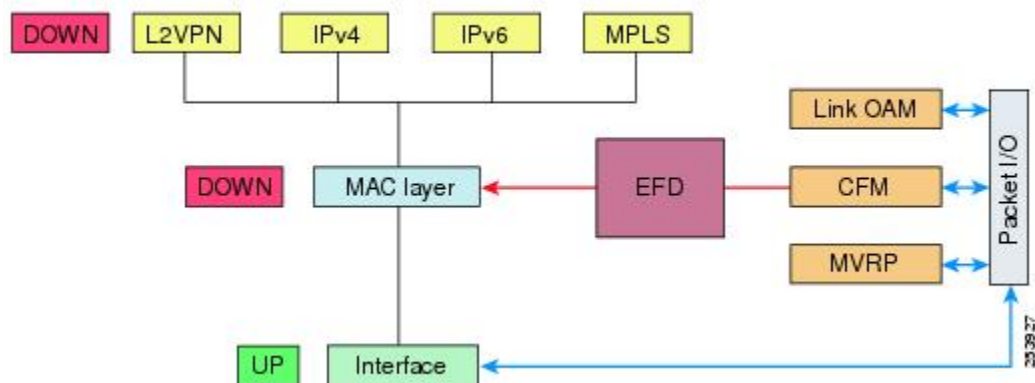
EFD changes this to allow EOAM to act as the line protocol for Ethernet interfaces. This allows EOAM to control the interface state so that if a EOAM defect (such as AIS or loss of continuity) is detected with an expected peer MEP, the interface can be shut down. This not only stops traffic flow, but also triggers actions in any higher-level protocols to route around the problem. For example, in the case of Layer 2 interfaces, the MAC table would be cleared and MSTP would reconverge. For Layer 3 interfaces, the ARP cache would be cleared and potentially the IGP would reconverge.



**Note** EFD can only be used for down MEPs. When EFD is used to shut down the interface, the EOAM frames continue to flow. This allows EOAM to detect when the problem has been resolved, and thus bring the interface backup automatically.

This figure shows EOAM detection of an error on one of its sessions EFD signaling an error to the corresponding MAC layer for the interface. This triggers the MAC to go to a down state, which further triggers all higher level protocols (Layer 2 pseudowires, IP protocols, and so on) to go down and also trigger a reconvergence where possible. As soon as EOAM detects there is no longer any error, it can signal to EFD and all protocols will once again go active.

**Figure 1: EOAM Error Detection and EFD Trigger**



## MIB Retrieval

MIB retrieval enables an OAM peer on one side of an interface to get the MIB variables from the remote side of the link. The MIB variables that are retrieved from the remote OAM peer are READ ONLY.

## Miswiring Detection (Cisco-Proprietary)

Miswiring Detection is a Cisco-proprietary feature that uses the 32-bit vendor field in every Information OAMPDU to identify potential miswiring cases.

## SNMP Traps

SNMP traps can be enabled or disabled on an Ethernet OAM interface.

# Configuring Ethernet OAM

Custom EOAM settings can be configured and shared on multiple interfaces by creating an EOAM profile in Ethernet configuration mode and then attaching the profile to individual interfaces. The profile configuration does not take effect until the profile is attached to an interface. After an EOAM profile is attached to an interface, individual EOAM features can be configured separately on the interface to override the profile settings when desired.

This section describes how to configure an EOAM profile and attach it to an interface in these procedures:

## Configuring an Ethernet OAM Profile

Perform these steps to configure an Ethernet OAM profile.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b>  RP/0/RP0/CPU0:router# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ethernet oam profile</b> <i>profile-name</i> <b>Example:</b>  RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1	Creates a new Ethernet Operations, Administration and Maintenance (OAM) profile and enters Ethernet OAM configuration mode.
<b>Step 3</b>	<b>link-monitor</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-eoam)# link-monitor	Enters the Ethernet OAM link monitor configuration mode.
<b>Step 4</b>	<b>symbol-period window</b> <i>window</i> <b>Example:</b>  RP/0/RP0/CPU0:router(config-eoam-lm)# symbol-period window 60000	(Optional) Configures the window size (in milliseconds) for an Ethernet OAM symbol-period error event. The IEEE 802.3 standard defines the window size as a number of symbols rather than a time duration. These two formats can be converted either way by using a knowledge of the interface speed and encoding.



	Command or Action	Purpose
		The range is 1000 to 60000. The default value is 1000.
<b>Step 5</b>	<b>symbol-period threshold low <i>threshold</i> high <i>threshold</i></b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# symbol-period threshold low 10000000 high 60000000</pre>	(Optional) Configures the thresholds (in symbols) that trigger an Ethernet OAM symbol-period error event. The high threshold is optional and is configurable only in conjunction with the low threshold. The range is 0 to 60000000. The default low threshold is 1.
<b>Step 6</b>		
<b>Step 7</b>	<b>frame window <i>window</i></b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame window 60</pre>	(Optional) Configures the frame window size (in milliseconds) of an OAM frame error event. The range is from 1000 to 60000. The default value is 1000.
<b>Step 8</b>	<b>frame threshold low <i>threshold</i> high <i>threshold</i></b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame threshold low 10000000 high 60000000</pre>	(Optional) Configures the thresholds (in symbols) that triggers an Ethernet OAM frame error event. The high threshold is optional and is configurable only in conjunction with the low threshold. The range is from 0 to 60000000. The default low threshold is 1.
<b>Step 9</b>	<b>frame-period window <i>window</i></b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-period window 60000 RP/0/RP0/CPU0:router(config-eoam-lm)# frame-period window milliseconds 60000</pre>	(Optional) Configures the window size (in milliseconds) for an Ethernet OAM frame-period error event. The IEEE 802.3 standard defines the window size as number of frames rather than a time duration. These two formats can be converted either way by using a knowledge of the interface speed. Note that the conversion assumes that all frames are of the minimum size. The range is from 100 to 60000. The default value is 1000. <b>Note</b> The only accepted values are multiples of the line card-specific polling interval, that is, 1000 milliseconds for most line cards.
<b>Step 10</b>	<b>frame-period threshold low <i>threshold</i> high <i>threshold</i></b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-period threshold ppm low 100 high 1000000</pre>	(Optional) Configures the thresholds (in errors per million frames ) that trigger an Ethernet OAM frame-period error event. The frame period window is defined in the IEEE specification as a number of received frames, in our implementation it is x milliseconds. The high threshold is optional and is configurable only in conjunction with the low threshold. The range is from 0 to 1000000.

	Command or Action	Purpose
		<p>The default low threshold is 1.</p> <p>To obtain the number of frames, the configured time interval is converted to a window size in frames using the interface speed. For example, for a 1Gbps interface, the IEEE defines minimum frame size as 512 bits. So, we get a maximum of approximately 1.5 million frames per second. If the window size is configured to be 8 seconds (8000ms) then this would give us a Window of 12 million frames in the specification's definition of Errored Frame Window.</p> <p>The thresholds for frame-period are measured in errors per million frames. Hence, if you configure a window of 8000ms (that is a window of 12 million frames) and a high threshold of 100, then the threshold would be crossed if there are 1200 errored frames in that period (that is, 100 per million for 12 million).</p>
<b>Step 11</b>	<p><b>frame-seconds window</b> <i>window</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-seconds window 900000</pre>	<p>(Optional) Configures the window size (in milliseconds) for the OAM frame-seconds error event.</p> <p>The range is 10000 to 900000.</p> <p>The default value is 6000.</p> <p><b>Note</b> The only accepted values are multiples of the line card-specific polling interval, that is, 1000 milliseconds for most line cards.</p>
<b>Step 12</b>	<p><b>frame-seconds threshold low</b> <i>threshold</i> <b>high</b> <i>threshold</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-seconds threshold low 3 threshold high 900</pre>	<p>(Optional) Configures the thresholds (in seconds) that trigger a frame-seconds error event. The high threshold value can be configured only in conjunction with the low threshold value.</p> <p>The range is 1 to 900</p> <p>The default value is 1.</p>
<b>Step 13</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# exit</pre>	Exits back to Ethernet OAM mode.
<b>Step 14</b>	<p><b>mib-retrieval</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# mib-retrieval</pre>	Enables MIB retrieval in an Ethernet OAM profile or on an Ethernet OAM interface.
<b>Step 15</b>	<p><b>connection timeout</b> <i>&lt;timeout&gt;</i></p> <p><b>Example:</b></p>	<p>Configures the connection timeout period for an Ethernet OAM session. as a multiple of the hello interval.</p> <p>The range is 2 to 30.</p>

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config-eoam)# connection timeout 30	The default value is 5.
<b>Step 16</b>	<b>hello-interval 1s</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-eoam)# hello-interval 1s	Configures the time interval between hello packets for an Ethernet OAM session. The default is 1 second (1s).
<b>Step 17</b>	<b>mode {active passive}</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-eoam)# mode passive	Configures the Ethernet OAM mode. The default is active.
<b>Step 18</b>	<b>require-remote mode {active passive}</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-eoam)# require-remote mode active	Requires that active mode or passive mode is configured on the remote end before the OAM session becomes active.
<b>Step 19</b>	<b>require-remote mib-retrieval</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-eoam)# require-remote mib-retrieval	Requires that MIB-retrieval is configured on the remote end before the OAM session becomes active.
<b>Step 20</b>	<b>action capabilities-conflict {disable   efd   error-disable-interface}</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-eoam)# action capabilities-conflict efd	Specifies the action that is taken on an interface when a capabilities-conflict event occurs. The default action is to create a syslog entry.  <b>Note</b> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 21</b>	<b>action critical-event {disable   error-disable-interface}</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-eoam)# action critical-event error-disable-interface	Specifies the action that is taken on an interface when a critical-event notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.  <b>Note</b> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>

	Command or Action	Purpose
Step 22	<p><b>action discovery-timeout</b> {disable   efd   error-disable-interface}</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action discovery-timeout efd</pre>	<p>Specifies the action that is taken on an interface when a connection timeout occurs. The default action is to create a syslog entry.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
Step 23	<p><b>action dying-gasp</b> {disable   error-disable-interface}</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action dying-gasp error-disable-interface</pre>	<p>Specifies the action that is taken on an interface when a dying-gasp notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
Step 24	<p><b>action high-threshold</b> {error-disable-interface   log}</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action high-threshold error-disable-interface</pre>	<p>Specifies the action that is taken on an interface when a high threshold is exceeded. The default is to take no action when a high threshold is exceeded.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>disable</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and take no action at the interface when the event occurs.</li> </ul>
Step 25	<p><b>action session-down</b> {disable   efd   error-disable-interface}</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action session-down efd</pre>	<p>Specifies the action that is taken on an interface when an Ethernet OAM session goes down.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
Step 26	<p><b>action session-up disable</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action session-up disable</pre>	<p>Specifies that no action is taken on an interface when an Ethernet OAM session is established. The default action is to create a syslog entry.</p>

	Command or Action	Purpose
		<p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 27</b>	<p><b>action uni-directional link-fault</b> {<b>disable</b>   <b>efd</b>   <b>error-disable-interface</b>}</p>	<p>Specifies the action that is taken on an interface when a link-fault notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 28</b>	<p><b>action wiring-conflict</b> {<b>disable</b>   <b>efd</b>   <b>log</b>}</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action session-down efd</pre>	<p>Specifies the action that is taken on an interface when a wiring-conflict event occurs. The default is to put the interface into error-disable state.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>error-disable-interface</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and put the interface into error-disable state when the event occurs.</li> </ul>
<b>Step 29</b>	<p><b>uni-directional link-fault detection</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# uni-directional link-fault detection</pre>	<p>Enables detection of a local, unidirectional link fault and sends notification of that fault to an Ethernet OAM peer.</p>
<b>Step 30</b>	<p><b>commit</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-if)# commit</pre>	<p>Saves the configuration changes to the running configuration file and remains within the configuration session.</p>
<b>Step 31</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-if)# end</pre>	<p>Ends the configuration session and exits to the EXEC mode.</p>

## Attaching an Ethernet OAM Profile to an Interface

Perform these steps to attach an Ethernet OAM profile to an interface:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b>  RP/0/RP0/CPU0:router# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>interface [FastEthernet   HundredGigE   TenGigE]</b> <i>interface-path-id</i> <b>Example:</b>  RP/0/RP0/CPU0:router(config)# interface TenGigE 0/1/0/0	Enters interface configuration mode and specifies the Ethernet interface name and notation <i>rack/slot/module/port</i> .  <b>Note</b> <ul style="list-style-type: none"> <li>The example indicates an 8-port 10-Gigabit Ethernet interface in modular services card slot 1.</li> </ul>
<b>Step 3</b>	<b>ethernet oam</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if)# ethernet oam	Enables Ethernet OAM and enters interface Ethernet OAM configuration mode.
<b>Step 4</b>	<b>profile profile-name</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if-eoam)# profile Profile_1	Attaches the specified Ethernet OAM profile ( <i>profile-name</i> ), and all of its configuration, to the interface.
<b>Step 5</b>	<b>commit</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if)# commit	Saves the configuration changes to the running configuration file and remains within the configuration session.
<b>Step 6</b>	<b>end</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if)# end	Ends the configuration session and exits to the EXEC mode.

## Configuring Ethernet OAM at an Interface and Overriding the Profile Configuration

Using an EOAM profile is an efficient way of configuring multiple interfaces with a common EOAM configuration. However, if you want to use a profile but also change the behavior of certain functions for a particular interface, then you can override the profile configuration. To override certain profile settings that are applied to an interface, you can configure that command in interface Ethernet OAM configuration mode to change the behavior for that interface.

In some cases, only certain keyword options are available in interface Ethernet OAM configuration due to the default settings for the command. For example, without any configuration of the **action** commands, several forms of the command have a default behavior of creating a syslog entry when a profile is created and applied

to an interface. Therefore, the **log** keyword is not available in Ethernet OAM configuration for these commands in the profile because it is the default behavior. However, the **log** keyword is available in Interface Ethernet OAM configuration if the default is changed in the profile configuration so you can retain the action of creating a syslog entry for a particular interface.

To see all of the default Ethernet OAM configuration settings, see the [Verifying the Ethernet OAM Configuration, on page 66](#).

To configure Ethernet OAM settings at an interface and override the profile configuration, perform these steps:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b>  RP/0/RP0/CPU0:router# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> [HundredGigE   TenGigE] <i>interface-path-id</i> <b>Example:</b>  RP/0/RP0/CPU0:router(config)# interface TenGigE 0/1/0/0	Enters interface configuration mode and specifies the Ethernet interface name and notation <i>rack/slot/module/port</i> .  <b>Note</b> <ul style="list-style-type: none"> <li>The example indicates an 8-port 10-Gigabit Ethernet interface in modular services card slot 1.</li> </ul>
<b>Step 3</b>	<b>ethernet oam</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if)# ethernet oam	Enables Ethernet OAM and enters interface Ethernet OAM configuration mode.
<b>Step 4</b>	<i>interface-Ethernet-OAM-command</i> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if-eoam)# action capabilities-conflict error-disable-interface	Configures a setting for an Ethernet OAM configuration command and overrides the setting for the profile configuration, where <i>interface-Ethernet-OAM-command</i> is one of the supported commands on the platform in interface Ethernet OAM configuration mode.
<b>Step 5</b>	<b>commit</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if)# commit	Saves the configuration changes to the running configuration file and remains within the configuration session.
<b>Step 6</b>	<b>end</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if)# end	Ends the configuration session and exits to the EXEC mode.

## Verifying the Ethernet OAM Configuration

Use the **show ethernet oam configuration** command to display the values for the Ethernet OAM configuration for a particular interface, or for all interfaces. The following example shows the default values for Ethernet OAM settings:

```
RP/0/RP0/CPU0:router# show ethernet oam configuration
Thu Aug  5 22:07:06.870 DST
GigabitEthernet0/4/0/0:
  Hello interval:                               1s
  Mib retrieval enabled:                        N
  Uni-directional link-fault detection enabled: N
  Configured mode:                             Active
  Connection timeout:                           5
  Symbol period window:                         0
  Symbol period low threshold:                  1
  Symbol period high threshold:                None
  Frame window:                                 1000
  Frame low threshold:                          1
  Frame high threshold:                        None
  Frame period window:                         1000
  Frame period low threshold:                   1
  Frame period high threshold:                 None
  Frame seconds window:                        60000
  Frame seconds low threshold:                  1
  Frame seconds high threshold:                None
  High threshold action:                       None
  Link fault action:                           Log
  Dying gasp action:                           Log
  Critical event action:                       Log
  Discovery timeout action:                     Log
  Capabilities conflict action:                 Log
  Wiring conflict action:                      Error-Disable
  Session up action:                           Log
  Session down action:                         Log
  Require remote mode:                         Ignore
  Require remote MIB retrieval:                 N
```

## Configuration Examples for Ethernet OAM

This section provides the following configuration examples:

### Configuring Ethernet OAM Features on an Individual Interface: Example

This example shows how to configure Ethernet OAM features on an individual interface:

```
configure
interface TenGigE 0/1/0/0
 ethernet oam
  link-monitor
  symbol-period window 60000
  symbol-period threshold ppm low 10000000 high 60000000
  frame window 60
  frame threshold ppm low 10000000 high 60000000
  frame-period window 60000
  frame-period threshold ppm low 100 high 12000000
```



```

frame-seconds window 900000
frame-seconds threshold low 3 high 900
exit
mib-retrieval
connection timeout 30
require-remote mode active
require-remote mib-retrieval
action link-fault error-disable-interface
action dying-gasp error-disable-interface
action critical-event error-disable-interface
action discovery-timeout error-disable-interface
action session-down error-disable-interface
action capabilities-conflict error-disable-interface
action wiring-conflict error-disable-interface

commit

```

## Configuring an Ethernet OAM Profile Globally: Example

This example shows how to configure an Ethernet OAM profile globally:

```

configure
ethernet oam profile Profile_1
link-monitor
symbol-period window 60000
symbol-period threshold ppm low 10000000 high 60000000
frame window 60
frame threshold ppm low 10000000 high 60000000
frame-period window 60000
frame-period threshold ppm low 100 high 12000000
frame-seconds window 900000
frame-seconds threshold low 3 high 900
exit
mib-retrieval
connection timeout 30
require-remote mode active
require-remote mib-retrieval
action dying-gasp error-disable-interface
action critical-event error-disable-interface
action discovery-timeout error-disable-interface
action session-down error-disable-interface
action capabilities-conflict error-disable-interface
action wiring-conflict error-disable-interface

commit

```

## Configuring Ethernet OAM Features to Override the Profile on an Individual Interface: Example

This example shows the configuration of Ethernet OAM features in a profile followed by an override of that configuration on an interface:

```

configure
ethernet oam profile Profile_1
mode passive
action dying-gasp disable
action critical-event disable
action discovery-timeout disable

```

```
    action session-up disable
    action session-down disable
    action capabilities-conflict disable
    action wiring-conflict disable

    commit

configure
interface TenGigE 0/1/0/0
  ethernet oam
  profile Profile_1
  mode active
  action dying-gasp log
  action critical-event log
  action discovery-timeout log
  action session-up log
  action session-down log
  action capabilities-conflict log
  action wiring-conflict log

  commit
```

## Clearing Ethernet OAM Statistics on an Interface: Example

This example shows how to clear Ethernet OAM statistics on an interface:

```
RP/0/RP0/CPU0:router# clear ethernet oam statistics interface gigabitethernet 0/1/5/1
```

## Enabling SNMP Server Traps on a Router: Example

This example shows how to enable SNMP server traps on a router:

```
configure
  snmp-server traps ethernet oam events
```

# Ethernet CFM

Table 14: Feature History Table

Feature Name	Release	Description
CFM on Bundle Member Link for Connectivity Check	Release 7.3.15	<p>This feature introduces support for Connectivity Fault Management (CFM) on bundle members. Earlier, network administrators managed networks by using the fault, configuration, account, performance, security model. CFM is one of a suite of the Ethernet OAM protocols, which uses a combination of keepalive packets and MAC-based pings, and traceroutes to detect faults in a network.</p> <p>With the CFM feature, you:</p> <ul style="list-style-type: none"> <li>• reduce operating expenses for service operators by reducing network faults and errors</li> <li>• provide end-to-end maintenance of networks</li> </ul>
Up MEP and Down MEP Support in CFM	Release 7.3.15	<p>This feature introduces Maintenance End Points (MEP) entities that you can configure in a domain.</p> <p>MEPs send either CFM frames from the interface where they are configured or CFM frames that are received on other interfaces.</p> <p>MEPs allow you to perform fault management and carry out performance checks.</p>

Ethernet Connectivity Fault Management (CFM) is a service-level OAM protocol that provides tools for monitoring and troubleshooting end-to-end Ethernet services per VLAN. This includes proactive connectivity monitoring, fault verification, and fault isolation. CFM uses standard Ethernet frames and can be run on any physical media that is capable of transporting Ethernet service frames. Unlike most other Ethernet protocols which are restricted to a single physical link, CFM frames can transmit across the entire end-to-end Ethernet network.

CFM is defined in two standards:

- IEEE 802.1ag—Defines the core features of the CFM protocol.

- ITU-T Y.1731—Redefines, but maintains compatibility with the features of IEEE 802.1ag, and defines some additional features.

Ethernet CFM supports these functions of ITU-T Y.1731:

- ETH-CC, ETH-RDI, ETH-LB, ETH-LT—These are equivalent to the corresponding features defined in IEEE 802.1ag.




---

**Note** The Linktrace responder procedures defined in IEEE 802.1ag are used rather than the procedures defined in Y.1731; however, these are interoperable.

---

- ETH-AIS—The reception of ETH-LCK messages is also supported.

### Limitations and Restrictions

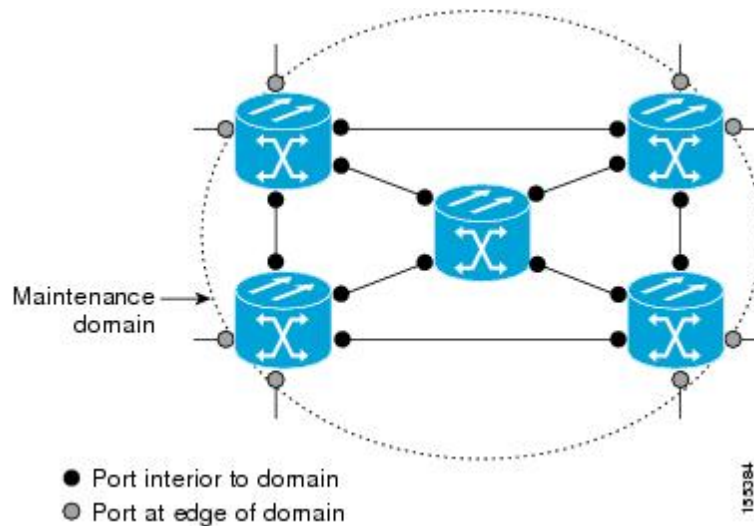
- The system supports only cross-connect.
- MIPs are not supported.
- Supports timer of 1s, 10s, 1m, 10m.
- Supports timer of 100ms, 1s, 10s, 1m, 10m for bundle members.
- L3 interfaces are not supported except for bundle members.
- Down MEPs are only supported for L2 cross-connect and bundle members.
- Multiple MEPs of different directions are not supported on the same interface or Xconnect.

## Maintenance Domains

To understand how the CFM maintenance model works, you need to understand these concepts and features:

A maintenance domain describes a management space for the purpose of managing and administering a network. A domain is owned and operated by a single entity and defined by the set of interfaces internal to it and at its boundary, as shown in this figure.

Figure 2: CFM Maintenance Domain



A maintenance domain is defined by the bridge ports that are provisioned within it. Domains are assigned maintenance levels, in the range of 0 to 7, by the administrator. The level of the domain is useful in defining the hierarchical relationships of multiple domains.

CFM maintenance domains allow different organizations to use CFM in the same network, but independently. For example, consider a service provider who offers a service to a customer, and to provide that service, they use two other operators in segments of the network. In this environment, CFM can be used in the following ways:

- The customer can use CFM between their CE devices, to verify and manage connectivity across the whole network.
- The service provider can use CFM between their PE devices, to verify and manage the services they are providing.
- Each operator can use CFM within their operator network, to verify and manage connectivity within their network.

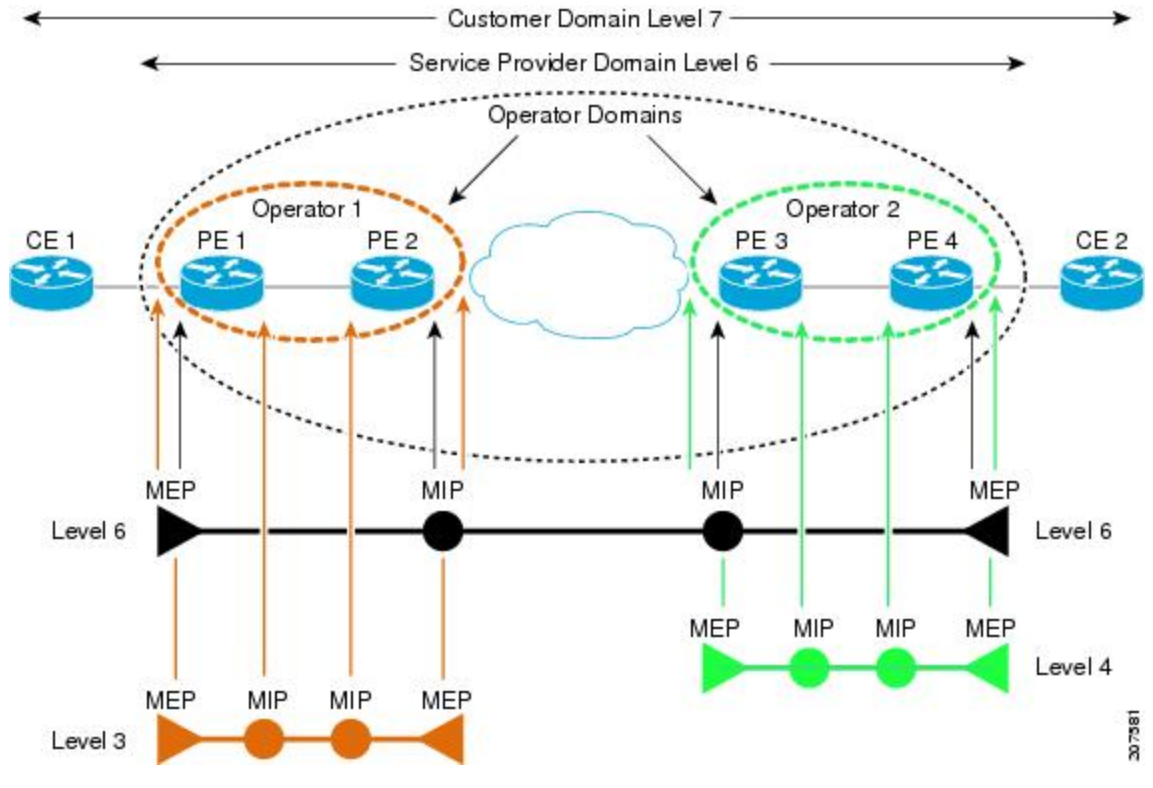
Each organization uses a different CFM maintenance domain.

This figure shows an example of the different levels of maintenance domains in a network.



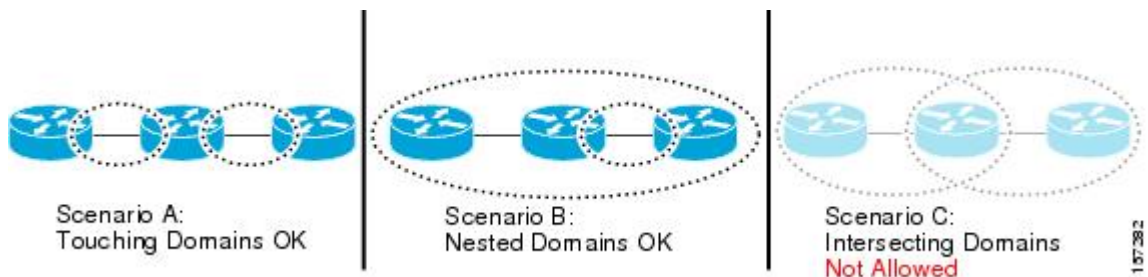
**Note** In CFM diagrams, the conventions are that triangles represent MEPs, pointing in the direction that the MEP sends CFM frames, and circles represent MIPs.

**Figure 3: Different CFM Maintenance Domains Across a Network**



To ensure that the CFM frames for each domain do not interfere with each other, each domain is assigned a maintenance level, between 0 and 7. Where domains are nested, as in this example, the encompassing domain must have a higher level than the domain it encloses. In this case, the domain levels must be negotiated between the organizations involved. The maintenance level is carried in all CFM frames that relate to that domain.

CFM maintenance domains may touch or nest, but cannot intersect. This figure illustrates the supported structure for touching and nested domains, and the unsupported intersection of domains.



## Services

A CFM service allows an organization to partition its CFM maintenance domain, according to the connectivity within the network. For example, if the network is divided into a number of virtual LANs (VLANs), a CFM service is created for each of these. CFM can then operate independently in each service. It is important that the CFM services match the network topology, so that CFM frames relating to one service cannot be received in a different service. For example, a service provider may use a separate CFM service for each of their customers, to verify and manage connectivity between that customer's end points.

A CFM service is always associated with the maintenance domain that it operates within, and therefore with that domain's maintenance level. All CFM frames relating to the service carry the maintenance level of the corresponding domain.



---

**Note** CFM Services are referred to as *Maintenance Associations* in IEEE 802.1ag and as *Maintenance Entity Groups* in ITU-T Y.1731.

---

## Maintenance Points

A CFM Maintenance Point (MP) is an instance of a particular CFM service on a specific interface. CFM only operates on an interface if there is a CFM maintenance point on the interface; otherwise, CFM frames are forwarded transparently through the interface.

A maintenance point is always associated with a particular CFM service, and therefore with a particular maintenance domain at a particular level. Maintenance points generally only process CFM frames at the same level as their associated maintenance domain. Frames at a higher maintenance level are always forwarded transparently, while frames at a lower maintenance level are normally dropped. This helps enforce the maintenance domain hierarchy, and ensures that CFM frames for a particular domain cannot leak out beyond the boundary of the domain.

There are following type(s) of MP(s):

- **Maintenance End Points (MEPs)**—Created at the edge of the domain. Maintenance end points (MEPs) are members of a particular service within a domain and are responsible for sourcing and sinking CFM frames. They periodically transmit continuity check messages and receive similar messages from other MEPs within their domain. They also transmit traceroute and loopback messages at the request of the administrator. MEPs are responsible for confining CFM messages within the domain.

## MEP and CFM Processing Overview

The boundary of a domain is an interface, rather than a bridge or host. Therefore, MEPs can be sub-divided into two categories:

- **Down MEPs**—Send CFM frames from the interface where they are configured, and process CFM frames received on that interface. Down MEPs transmit AIS messages upward (toward the cross-connect).
- **Up MEPs**—Send frames into the bridge relay function, as if they had been received on the interface where the MEP is configured. They process CFM frames that have been received on other interfaces, and have been switched through the bridge relay function as if they are going to be sent out of the interface where the MEP is configured. Up MEPs transmit AIS messages downward (toward the wire). However,

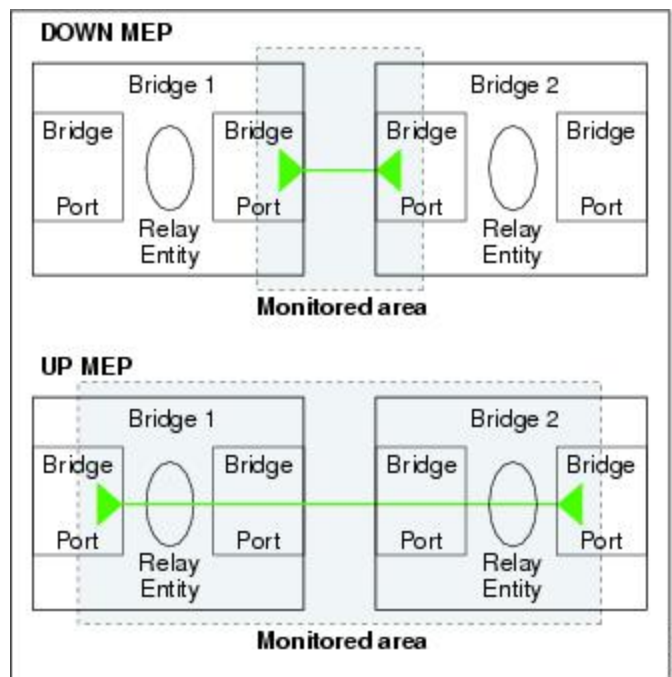
AIS packets are only sent when there is a MIP configured on the same interface as the MEP and at the level of the MIP.



- Note**
- The terms *Down MEP* and *Up MEP* are defined in the IEEE 802.1ag and ITU-T Y.1731 standards, and refer to the direction that CFM frames are sent from the MEP. The terms should not be confused with the operational status of the MEP.
  - The router only supports the “Down MEP level < Up MEP level” configuration.

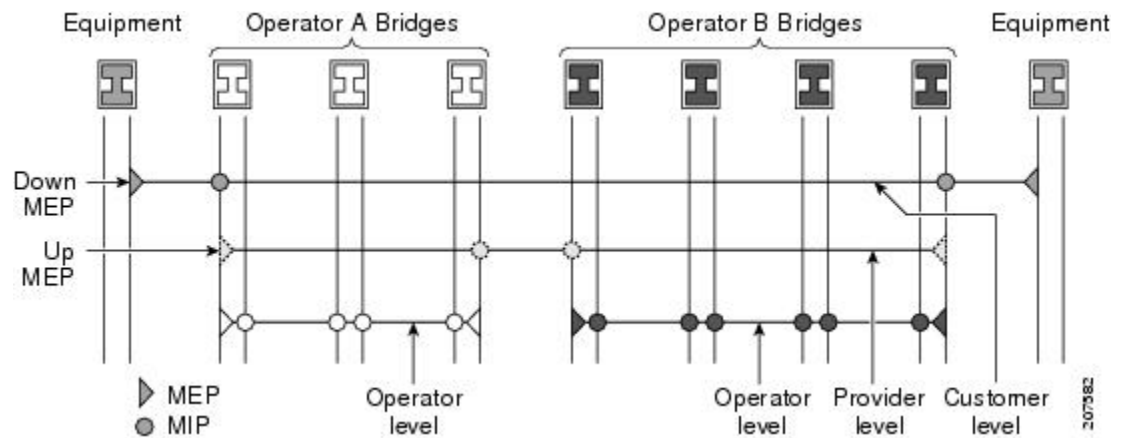
This figure illustrates the monitored areas for Down and Up MEPs.

**Figure 4: Monitored Areas for Down and Up MEPs**



This figure shows maintenance points at different levels. Because domains are allowed to nest but not intersect (see ), a MEP at a low level always corresponds with a MEP at a higher level.





Up MEPs can only exist on switched (Layer 2) interfaces, because they send and receive frames from the bridge relay function. Down MEPs can be created on switched (Layer 2) interfaces.

MEPs continue to operate normally if the interface they are created on is blocked by the Spanning Tree Protocol (STP); that is, CFM frames at the level of the MEP continue to be sent and received, according to the direction of the MEP. MEPs never allow CFM frames at the level of the MEP to be forwarded, so the STP block is maintained.



**Note** A separate set of CFM maintenance levels is created every time a VLAN tag is pushed onto the frame. Therefore, if CFM frames are received on an interface which pushes an additional tag, so as to “tunnel” the frames over part of the network, the CFM frames will not be processed by any MPs within the tunnel, even if they are at the same level. For example, if a CFM MP is created on an interface with an encapsulation that matches a single VLAN tag, any CFM frames that are received at the interface that have two VLAN tags will be forwarded transparently, regardless of the CFM level.

## CFM Protocol Messages

The CFM protocol consists of a number of different message types, with different purposes. All CFM messages use the CFM EtherType, and carry the CFM maintenance level for the domain to which they apply.

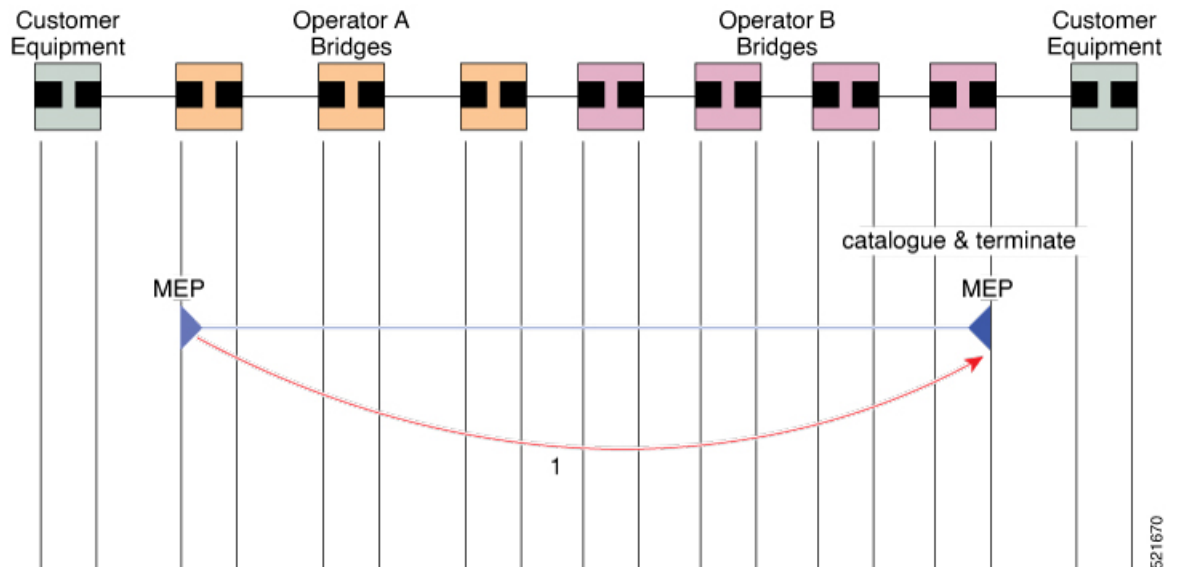
This section describes the following CFM messages:

### Continuity Check (IEEE 802.1ag and ITU-T Y.1731)

Continuity Check Messages (CCMs) are “heartbeat” messages exchanged periodically between all the MEPs in a service. Each MEP sends out multicast CCMs, and receives CCMs from all the other MEPs in the service—these are referred to as *peer MEPs*. This allows each MEP to discover its peer MEPs, and to verify that there is connectivity between them.

MIPs also receive CCMs. MIPs use the information to build a MAC learning database that is used when responding to Linktrace. For more information about Linktrace, see the [Linktrace \(IEEE 802.1ag and ITU-T Y.1731\)](#).

Figure 5: Continuity Check Message Flow



All the MEPs in a service must transmit CCMs at the same interval. IEEE 802.1ag defines the following possible intervals that can be used:

- 100 ms (only supported on bundle members)
- 1 s
- 10 s
- 1 minute
- 10 minutes

A MEP detects a loss of connectivity with one of its peer MEPs when some number of CCMs are missed. This occurs when sufficient time has passed during which a certain number of CCMs were expected, given the CCM interval. This number is called the *loss threshold*, and is usually set to 3.

With the exception of bundle members, CFM is supported only on interfaces that have Layer 2 transport feature enabled.

CCM messages carry a variety of information that allows different defects to be detected in the service. This information includes:

- A configured identifier for the domain of the transmitting MEP. This is referred to as the Maintenance Domain Identifier (MDID).
- A configured identifier for the service of the transmitting MEP. This is referred to as the Short MA Name (SMAN). Together, the MDID and the SMAN make up the Maintenance Association Identifier (MAID). The MAID must be configured identically on every MEP in the service.
- These are restrictions on the type of MAID that are supported for sessions with time interval of less than 1 minute. The MAID supports two types of formats on offloaded MEPs:
  - No Domain Name Format
  - MD Name Format = 1-NoDomainName

- Short MA Name Format = 3 - 2 bytes integer value
- Short MA Name Length = 2 - fixed length
- Short MA Name = 2 bytes of integer
- 1731 Maid Format
  - MD Name Format = 1-NoDomainName
  - MA Name Format(MEGID Format) = 32
  - MEGID Length = 13 - fixed length
  - MEGID(ICCCode) = 6 Bytes
  - MEGID(UMC) = 7 Bytes
  - ITU Carrier Code (ICC) - Number of different configurable ICC code - 15 (for each NPU)
  - Unique MEG ID Code (UMC) - 4

Maintenance Association Identifier (MAID) comprises of the Maintenance Domain Identifier (MDID) and Short MA Name (SMAN). MDID only supports **null** value and SMAN only supports ITU Carrier Code (ICC) or a numerical. No other values are supported.

- An example for configuring domain ID null is: **ethernet cfm domain SMB level 3 id null**
- An example for configuring SMAN is: **ethernet cfm domain SMB level 3 id null service 901234AB xconnect group 99999 p2p 99999 id number 1**
- A configured numeric identifier for the MEP (the MEP ID). Each MEP in the service must be configured with a different MEP ID.
- Dynamic Remote MEPs are not supported for MEPs with less than 1 min interval. You must configure MEP CrossCheck for all such MEPs.
- Sequence numbering is not supported for MEPs with less than 1 minute interval.
- In a Remote Defect Indication (RDI), each MEP includes this in the CCMs it is sending, if it has detected a defect relating to the CCMs it is receiving. This notifies all the MEPs in the service that a defect has been detected somewhere in the service.
- The interval at which CCMs are being transmitted.
- CCM Tx/Rx statistics counters are not supported for MEPs with less than 1 minute intervals.
- Sender TLV and Cisco Proprietary TLVs are not supported for MEPs with less than 1 minute intervals.
- The status of the interface where the MEP is operating, for example, whether the interface is up, down, STP blocked, and so on.




---

**Note** The status of the interface (up/down) should not be confused with the direction of any MEPs on the interface (Up MEPs/Down MEPs).

---

These defects can be detected from the received CCMs:

- Interval mismatch: The CCM interval in the received CCM does not match the interval that the MEP is sending CCMs.
- Level mismatch: A MEP has received a CCM carrying a lower maintenance level than the MEPs own level.
- Loop: A CCM is received with the source MAC address equal to the MAC address of the interface where the MEP is operating.
- Configuration error: A CCM is received with the same MEP ID as the MEP ID configured for the receiving MEP.
- Cross-connect: A CCM is received with a MAID that does not match the locally configured MAID. This generally indicates a VLAN misconfiguration within the network, such that CCMs from one service are leaking into a different service.
- Peer interface down: A CCM is received that indicates the interface on the peer is down.
- Remote defect indication: A CCM is received carrying a remote defect indication.



---

**Note** This defect does not cause the MEP to include a remote defect indication in the CCMs that it is sending.

---

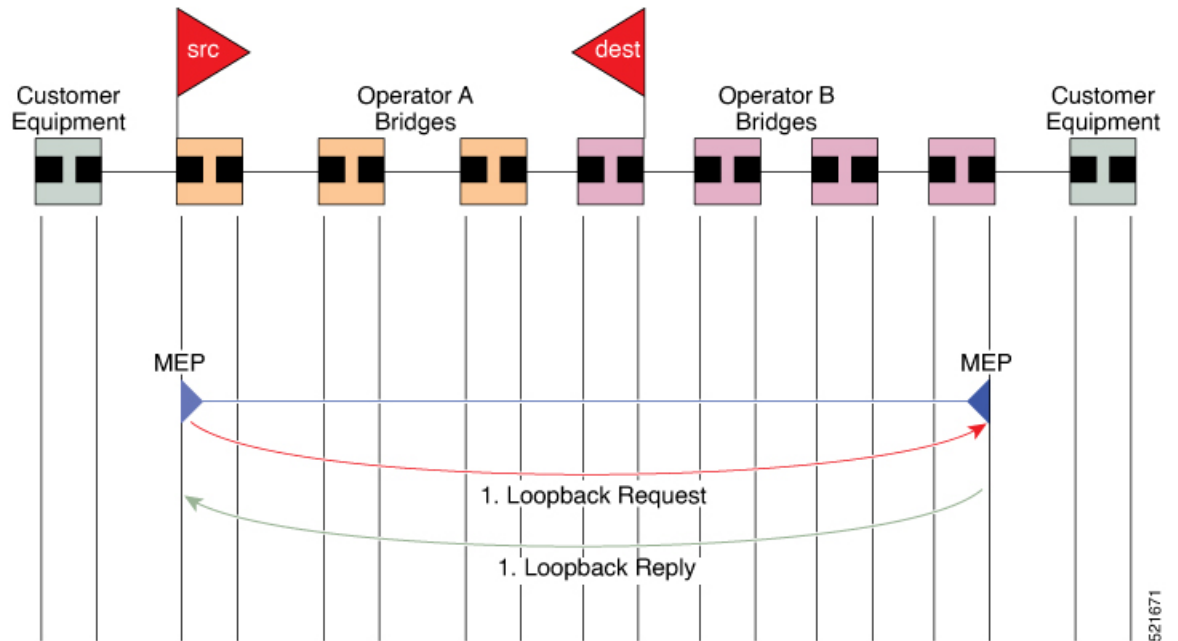
Out-of-sequence CCMs can also be detected by monitoring the sequence number in the received CCMs from each peer MEP. However, this is not considered a CCM defect.

## Loopback (IEEE 802.1ag and ITU-T Y.1731)

Loopback Messages (LBM) and Loopback Replies (LBR) are used to verify connectivity between a local MEP and a particular remote MP. At the request of the administrator, a local MEP sends unicast LBMs to the remote MP. On receiving each LBM, the target maintenance point sends an LBR back to the originating MEP. Loopback indicates whether the destination is reachable or not—it does not allow hop-by-hop discovery of the path. It is similar in concept to an ICMP Echo (ping). Since loopback messages are destined for unicast addresses, they are forwarded like normal data traffic, while observing the maintenance levels. At each device that the loopback reaches, if the outgoing interface is known (in the bridge's forwarding database), then the frame is sent out on that interface. If the outgoing interface is not known, then the message is flooded on all interfaces.

This figure shows an example of CFM loopback message flow between a MEP and MEP.

Figure 6: Loopback Messages



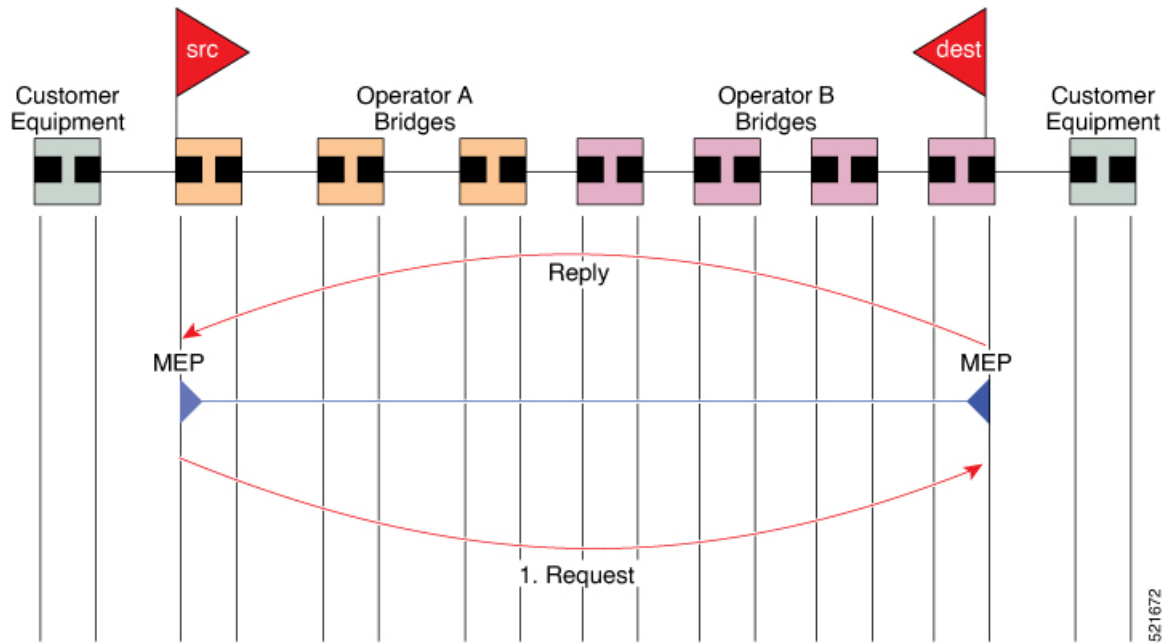
Loopback messages can be padded with user-specified data. This allows data corruption to be detected in the network. They also carry a sequence number which allows for out-of-order frames to be detected.

## Linktrace (IEEE 802.1ag and ITU-T Y.1731)

Linktrace Messages (LTM) and Linktrace Replies (LTR) are used to track the path (hop-by-hop) to a unicast destination MAC address. At the request of the operator, a local MEP sends an LTM. Each hop where there is a maintenance point sends an LTR back to the originating MEP. This allows the administrator to discover connectivity data about the path. It is similar in concept to IP traceroute, although the mechanism is different. In IP traceroute, successive probes are sent, whereas CFM Linktrace uses a single LTM which is forwarded by each MP in the path. LTMs are multicast, and carry the unicast target MAC address as data within the frame. They are intercepted at each hop where there is a maintenance point, and either retransmitted or dropped to discover the unicast path to the target MAC address.

This figure shows an example of CFM linktrace message flow between MEPs and MEPs.

Figure 7: Linktrace Message Flow



The linktrace mechanism is designed to provide useful information even after a network failure. This allows it to be used to locate failures, for example after a loss of continuity is detected. To achieve this, each MP maintains a CCM Learning Database. This maps the source MAC address for each received CCM to the interface through which the CCM was received. It is similar to a typical bridge MAC learning database, except that it is based only on CCMs and it times out much more slowly—on the order of days rather than minutes.



**Note** In IEEE 802.1ag, the CCM Learning Database is referred to as the MIP CCM Database. However, it applies to both MIPs and MEPs.

In IEEE 802.1ag, when an MP receives an LTM message, it determines whether to send a reply using the following steps:

1. The target MAC address in the LTM is looked up in the bridge MAC learning table. If the MAC address is known, and therefore the egress interface is known, then an LTR is sent.
2. If the MAC address is not found in the bridge MAC learning table, then it is looked up in the CCM learning database. If it is found, then an LTR is sent.
3. If the MAC address is not found, then no LTR is sent (and the LTM is not forwarded).

If the target MAC has never been seen previously in the network, the linktrace operation will not produce any results.



**Note** IEEE 802.1ag and ITU-T Y.1731 define slightly different linktrace mechanisms. In particular, the use of the CCM learning database and the algorithm described above for responding to LTM messages are specific to IEEE 802.1ag. IEEE 802.1ag also specifies additional information that can be included in LTRs. Regardless of the differences, the two mechanisms are interoperable.

## Configurable Logging

CFM supports logging of various conditions to syslog. Logging can be enabled independently for each service, and when the following conditions occur:

- New peer MEPs are detected, or loss of continuity with a peer MEP occurs.
- Changes to the CCM defect conditions are detected.
- Cross-check “missing” or “unexpected” conditions are detected.
- AIS condition detected (AIS messages received) or cleared (AIS messages no longer received).
- EFD used to shut down an interface, or bring it back up.

## How to Configure Ethernet OAM

This section provides these configuration procedures:

### Configuring Ethernet OAM

Custom EOAM settings can be configured and shared on multiple interfaces by creating an EOAM profile in Ethernet configuration mode and then attaching the profile to individual interfaces. The profile configuration does not take effect until the profile is attached to an interface. After an EOAM profile is attached to an interface, individual EOAM features can be configured separately on the interface to override the profile settings when desired.

This section describes how to configure an EOAM profile and attach it to an interface in these procedures:

### Configuring an Ethernet OAM Profile

Perform these steps to configure an Ethernet OAM profile.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>ethernet oam profile</b> <i>profile-name</i> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config)# ethernet oam profile Profile_1</pre>	Creates a new Ethernet Operations, Administration and Maintenance (OAM) profile and enters Ethernet OAM configuration mode.
<b>Step 3</b>	<b>link-monitor</b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam)# link-monitor</pre>	Enters the Ethernet OAM link monitor configuration mode.
<b>Step 4</b>	<b>symbol-period window</b> <i>window</i> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# symbol-period window 60000</pre>	(Optional) Configures the window size (in milliseconds) for an Ethernet OAM symbol-period error event. The IEEE 802.3 standard defines the window size as a number of symbols rather than a time duration. These two formats can be converted either way by using a knowledge of the interface speed and encoding.  The range is 1000 to 60000.  The default value is 1000.
<b>Step 5</b>	<b>symbol-period threshold low</b> <i>threshold</i> <b>high</b> <i>threshold</i> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# symbol-period threshold low 10000000 high 60000000</pre>	(Optional) Configures the thresholds (in symbols) that trigger an Ethernet OAM symbol-period error event. The high threshold is optional and is configurable only in conjunction with the low threshold.  The range is 0 to 60000000.  The default low threshold is 1.
<b>Step 6</b>		
<b>Step 7</b>	<b>frame window</b> <i>window</i> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame window 60</pre>	(Optional) Configures the frame window size (in milliseconds) of an OAM frame error event.  The range is from 1000 to 60000.  The default value is 1000.
<b>Step 8</b>	<b>frame threshold low</b> <i>threshold</i> <b>high</b> <i>threshold</i> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame threshold low 10000000 high 60000000</pre>	(Optional) Configures the thresholds (in symbols) that triggers an Ethernet OAM frame error event. The high threshold is optional and is configurable only in conjunction with the low threshold.  The range is from 0 to 60000000.  The default low threshold is 1.
<b>Step 9</b>	<b>frame-period window</b> <i>window</i> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-period window 60000</pre>	(Optional) Configures the window size (in milliseconds) for an Ethernet OAM frame-period error event. The IEEE 802.3 standard defines the window size as number of frames rather than a time duration. These two formats can be converted either way by using a knowledge of the



	Command or Action	Purpose
	<pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-period window milliseconds 60000</pre>	<p>interface speed. Note that the conversion assumes that all frames are of the minimum size.</p> <p>The range is from 100 to 60000.</p> <p>The default value is 1000.</p> <p><b>Note</b> The only accepted values are multiples of the line card-specific polling interval, that is, 1000 milliseconds for most line cards.</p>
<b>Step 10</b>	<p><b>frame-period threshold low</b><i>threshold</i> <b>high</b> <i>threshold</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-period threshold ppm low 100 high 1000000</pre>	<p>(Optional) Configures the thresholds (in errors per million frames ) that trigger an Ethernet OAM frame-period error event. The frame period window is defined in the IEEE specification as a number of received frames, in our implementation it is x milliseconds. The high threshold is optional and is configurable only in conjunction with the low threshold.</p> <p>The range is from 0 to 1000000.</p> <p>The default low threshold is 1.</p> <p>To obtain the number of frames, the configured time interval is converted to a window size in frames using the interface speed. For example, for a 1Gbps interface, the IEEE defines minimum frame size as 512 bits. So, we get a maximum of approximately 1.5 million frames per second. If the window size is configured to be 8 seconds (8000ms) then this would give us a Window of 12 million frames in the specification's definition of Errored Frame Window.</p> <p>The thresholds for frame-period are measured in errors per million frames. Hence, if you configure a window of 8000ms (that is a window of 12 million frames) and a high threshold of 100, then the threshold would be crossed if there are 1200 errored frames in that period (that is, 100 per million for 12 million).</p>
<b>Step 11</b>	<p><b>frame-seconds window</b> <i>window</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-seconds window 900000</pre>	<p>(Optional) Configures the window size (in milliseconds) for the OAM frame-seconds error event.</p> <p>The range is 10000 to 900000.</p> <p>The default value is 6000.</p> <p><b>Note</b> The only accepted values are multiples of the line card-specific polling interval, that is, 1000 milliseconds for most line cards.</p>
<b>Step 12</b>	<p><b>frame-seconds threshold low</b> <i>threshold</i> <b>high</b> <i>threshold</i></p> <p><b>Example:</b></p>	<p>(Optional) Configures the thresholds (in seconds) that trigger a frame-seconds error event. The high threshold</p>

	Command or Action	Purpose
	<pre>RP/0/RP0/CPU0:router(config-eoam-lm)# frame-seconds threshold low 3 threshold high 900</pre>	<p>value can be configured only in conjunction with the low threshold value.</p> <p>The range is 1 to 900</p> <p>The default value is 1.</p>
<b>Step 13</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam-lm)# exit</pre>	Exits back to Ethernet OAM mode.
<b>Step 14</b>	<p><b>mib-retrieval</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# mib-retrieval</pre>	Enables MIB retrieval in an Ethernet OAM profile or on an Ethernet OAM interface.
<b>Step 15</b>	<p><b>connection timeout &lt;timeout&gt;</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# connection timeout 30</pre>	<p>Configures the connection timeout period for an Ethernet OAM session, as a multiple of the hello interval.</p> <p>The range is 2 to 30.</p> <p>The default value is 5.</p>
<b>Step 16</b>	<p><b>hello-interval 1s</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# hello-interval 1s</pre>	Configures the time interval between hello packets for an Ethernet OAM session. The default is 1 second (1s).
<b>Step 17</b>	<p><b>mode {active passive}</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# mode passive</pre>	Configures the Ethernet OAM mode. The default is active.
<b>Step 18</b>	<p><b>require-remote mode {active passive}</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# require-remote mode active</pre>	Requires that active mode or passive mode is configured on the remote end before the OAM session becomes active.
<b>Step 19</b>	<p><b>require-remote mib-retrieval</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# require-remote mib-retrieval</pre>	Requires that MIB-retrieval is configured on the remote end before the OAM session becomes active.
<b>Step 20</b>	<p><b>action capabilities-conflict {disable   efd   error-disable-interface}</b></p> <p><b>Example:</b></p>	Specifies the action that is taken on an interface when a capabilities-conflict event occurs. The default action is to create a syslog entry.

	Command or Action	Purpose
	<pre>RP/0/RP0/CPU0:router (config-eoam)# action capabilities-conflict efd</pre>	<p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 21</b>	<p><b>action critical-event {disable   error-disable-interface}</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router (config-eoam)# action critical-event error-disable-interface</pre>	<p>Specifies the action that is taken on an interface when a critical-event notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 22</b>	<p><b>action discovery-timeout {disable   efd   error-disable-interface}</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router (config-eoam)# action discovery-timeout efd</pre>	<p>Specifies the action that is taken on an interface when a connection timeout occurs. The default action is to create a syslog entry.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 23</b>	<p><b>action dying-gasp {disable   error-disable-interface}</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router (config-eoam)# action dying-gasp error-disable-interface</pre>	<p>Specifies the action that is taken on an interface when a dying-gasp notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 24</b>	<p><b>action high-threshold {error-disable-interface   log}</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router (config-eoam)# action high-threshold error-disable-interface</pre>	<p>Specifies the action that is taken on an interface when a high threshold is exceeded. The default is to take no action when a high threshold is exceeded.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>disable</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and take no action at the interface when the event occurs.</li> </ul>

	Command or Action	Purpose
<b>Step 25</b>	<p><b>action session-down {disable   efd   error-disable-interface}</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action session-down efd</pre>	<p>Specifies the action that is taken on an interface when an Ethernet OAM session goes down.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 26</b>	<p><b>action session-up disable</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action session-up disable</pre>	<p>Specifies that no action is taken on an interface when an Ethernet OAM session is established. The default action is to create a syslog entry.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 27</b>	<p><b>action uni-directional link-fault {disable   efd   error-disable-interface}</b></p>	<p>Specifies the action that is taken on an interface when a link-fault notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>log</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.</li> </ul>
<b>Step 28</b>	<p><b>action wiring-conflict {disable   efd   log}</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# action session-down efd</pre>	<p>Specifies the action that is taken on an interface when a wiring-conflict event occurs. The default is to put the interface into error-disable state.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you change the default, the <b>error-disable-interface</b> keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and put the interface into error-disable state when the event occurs.</li> </ul>
<b>Step 29</b>	<p><b>uni-directional link-fault detection</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-eoam)# uni-directional link-fault detection</pre>	<p>Enables detection of a local, unidirectional link fault and sends notification of that fault to an Ethernet OAM peer.</p>

	Command or Action	Purpose
<b>Step 30</b>	<b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# commit	Saves the configuration changes to the running configuration file and remains within the configuration session.
<b>Step 31</b>	<b>end</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# end	Ends the configuration session and exits to the EXEC mode.

## Attaching an Ethernet OAM Profile to an Interface

Perform these steps to attach an Ethernet OAM profile to an interface:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>interface [FastEthernet   HundredGigE   TenGigE]</b> <i>interface-path-id</i> <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface TenGigE 0/1/0/0	Enters interface configuration mode and specifies the Ethernet interface name and notation <i>rack/slot/module/port</i> . <b>Note</b> <ul style="list-style-type: none"> <li>The example indicates an 8-port 10-Gigabit Ethernet interface in modular services card slot 1.</li> </ul>
<b>Step 3</b>	<b>ethernet oam</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ethernet oam	Enables Ethernet OAM and enters interface Ethernet OAM configuration mode.
<b>Step 4</b>	<b>profile profile-name</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if-eoam)# profile Profile_1	Attaches the specified Ethernet OAM profile ( <i>profile-name</i> ), and all of its configuration, to the interface.
<b>Step 5</b>	<b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# commit	Saves the configuration changes to the running configuration file and remains within the configuration session.

	Command or Action	Purpose
<b>Step 6</b>	<b>end</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# end	Ends the configuration session and exits to the EXEC mode.

## Configuring Ethernet OAM at an Interface and Overriding the Profile Configuration

Using an EOAM profile is an efficient way of configuring multiple interfaces with a common EOAM configuration. However, if you want to use a profile but also change the behavior of certain functions for a particular interface, then you can override the profile configuration. To override certain profile settings that are applied to an interface, you can configure that command in interface Ethernet OAM configuration mode to change the behavior for that interface.

In some cases, only certain keyword options are available in interface Ethernet OAM configuration due to the default settings for the command. For example, without any configuration of the **action** commands, several forms of the command have a default behavior of creating a syslog entry when a profile is created and applied to an interface. Therefore, the **log** keyword is not available in Ethernet OAM configuration for these commands in the profile because it is the default behavior. However, the **log** keyword is available in Interface Ethernet OAM configuration if the default is changed in the profile configuration so you can retain the action of creating a syslog entry for a particular interface.

To see all of the default Ethernet OAM configuration settings, see the [Verifying the CFM Configuration](#).

To configure Ethernet OAM settings at an interface and override the profile configuration, perform these steps:

### SUMMARY STEPS

1. **configure**
2. **interface** [HundredGigE | TenGigE] *interface-path-id*
3. **ethernet oam**
4. *interface-Ethernet-OAM-command*
5. **commit**
6. **end**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> [HundredGigE   TenGigE] <i>interface-path-id</i> <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface TenGigE 0/1/0/0	Enters interface configuration mode and specifies the Ethernet interface name and notation <i>rack/slot/module/port</i> .  <b>Note</b> <ul style="list-style-type: none"> <li>• The example indicates an 8-port 10-Gigabit Ethernet interface in modular services card slot 1.</li> </ul>

	Command or Action	Purpose
Step 3	<b>ethernet oam</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ethernet oam	Enables Ethernet OAM and enters interface Ethernet OAM configuration mode.
Step 4	<b>interface-Ethernet-OAM-command</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if-eoam)# action capabilities-conflict error-disable-interface	Configures a setting for an Ethernet OAM configuration command and overrides the setting for the profile configuration, where <i>interface-Ethernet-OAM-command</i> is one of the supported commands on the platform in interface Ethernet OAM configuration mode.
Step 5	<b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# commit	Saves the configuration changes to the running configuration file and remains within the configuration session.
Step 6	<b>end</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# end	Ends the configuration session and exits to the EXEC mode.

## Verifying the Ethernet OAM Configuration

Use the **show ethernet oam configuration** command to display the values for the Ethernet OAM configuration for a particular interface, or for all interfaces. The following example shows the default values for Ethernet OAM settings:

```
RP/0/RP0/CPU0:router# show ethernet oam configuration
Thu Aug  5 22:07:06.870 DST
GigabitEthernet0/4/0/0:
  Hello interval:                               1s
  Mib retrieval enabled:                         N
  Uni-directional link-fault detection enabled:  N
  Configured mode:                              Active
  Connection timeout:                            5
  Symbol period window:                          0
  Symbol period low threshold:                   1
  Symbol period high threshold:                  None
  Frame window:                                  1000
  Frame low threshold:                           1
  Frame high threshold:                          None
  Frame period window:                           1000
  Frame period low threshold:                     1
  Frame period high threshold:                    None
  Frame seconds window:                          60000
  Frame seconds low threshold:                    1
  Frame seconds high threshold:                   None
  High threshold action:                         None
  Link fault action:                             Log
  Dying gasp action:                             Log
  Critical event action:                         Log
  Discovery timeout action:                       Log
  Capabilities conflict action:                  Log
```

```

Wiring conflict action:      Error-Disable
Session up action:          Log
Session down action:        Log
Require remote mode:        Ignore
Require remote MIB retrieval: N
    
```

## Configuring Ethernet CFM

To configure Ethernet CFM, perform the following tasks:



**Note** CFM is not supported for the following:

- L3 Interfaces and Sub-Interfaces
- Bridge Domain, Release 7.3.1 and earlier
- VPLS, Release 7.3.1 and earlier

## Configuring a CFM Maintenance Domain

To configure a CFM maintenance domain, perform the following steps:

### SUMMARY STEPS

1. **configure**
2. **ethernet cfm**
3. **domain** *domain-name* **level** *level-value* [**id** [**null**] [**dns** *DNS-name*] [**mac** *H.H.H*] [**string** *string*] ]
4. **traceroute cache hold-time** *minutes* **size** *entries*
5. **end** or **commit**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b>  RP/0/RP0/CPU0:router# <code>configure</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ethernet cfm</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config)# <code>ethernet cfm</code>	Enters Ethernet Connectivity Fault Management (CFM) configuration mode.
<b>Step 3</b>	<b>domain</b> <i>domain-name</i> <b>level</b> <i>level-value</i> [ <b>id</b> [ <b>null</b> ] [ <b>dns</b> <i>DNS-name</i> ] [ <b>mac</b> <i>H.H.H</i> ] [ <b>string</b> <i>string</i> ] ] <b>Example:</b>	Creates and names a container for all domain configurations and enters CFM domain configuration mode.  The level must be specified.



	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1	The <b>id</b> is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames. If the MDID is not specified, the domain name is used as the MDID by default.
<b>Step 4</b>	<b>traceroute cache hold-time <i>minutes</i> size <i>entries</i></b>  <b>Example:</b>  RP/0/RP0/CPU0:router(config-cfm)# traceroute cache hold-time 1 size 3000	(Optional) Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries. The default is 100 minutes and 100 entries.
<b>Step 5</b>	<b>end or commit</b>  <b>Example:</b>  RP/0/RP0/CPU0:router(config-cfm-dmn)# commit	Saves configuration changes.  <ul style="list-style-type: none"> <li>When you use the <b>end</b> command, the system prompts you to commit changes:   <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> </li> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Configuring Services for a CFM Maintenance Domain

You can configure up to 50 CFM sessions per line card or 50 CFM sessions per fixed-port router. The system supports 50 CFM sessions on bundles.

CFM services for a maintenance domain. To configure services for a CFM maintenance domain, perform the following steps:

### SUMMARY STEPS

- configure**
- ethernet cfm**
- domain *domain-name* level *level-value* [*id* [null] [*dns* *DNS-name*] [*mac* *H.H.H*] [*string* *string*]]**
- service *service-name* {*down-meps* | *xconnect* group *xconnect-group-name* p2p *xconnect-name*} [*id* [*icc-based* *icc-string* *umc-string*]] [ [*number* *number*]]**

## 5. end or commit

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>ethernet cfm</b> <b>Example:</b> RP/0/RP0/CPU0:router(config)# ethernet cfm	Enters Ethernet CFM configuration mode.
<b>Step 3</b>	<b>domain</b> <i>domain-name</i> <b>level</b> <i>level-value</i> [ <b>id</b> [ <b>null</b> ] [ <b>dns</b> <i>DNS-name</i> ] [ <b>mac</b> <i>H.H.H</i> ] [ <b>string</b> <i>string</i> ] ] <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1	<p>Creates and names a container for all domain configurations at a specified maintenance level, and enters CFM domain configuration mode.</p> <p>The <b>id</b> is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames. If the MDID is not specified, the domain name is used as the MDID by default.</p>
<b>Step 4</b>	<b>service</b> <i>service-name</i> { <b>down-meps</b>   <b>xconnect</b> <b>group</b> <i>xconnect-group-name</i> <b>p2p</b> <i>xconnect-name</i> } [ <b>id</b> [ <b>icc-based</b> <i>icc-string umc-string</i> ]   [ <b>number</b> <i>number</i> ] ] <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn)# service xconnect group X1	<p>Configures and associates a service with the domain and enters CFM domain service configuration mode. You can specify that the service is used only for down MEPs.</p> <p>The <b>id</b> sets the short MA name.</p>
<b>Step 5</b>	<b>end</b> or <b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# commit	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>When you use the <b>end</b> command, the system prompts you to commit changes:   <pre>Uncommitted changes found, commit them before   exiting(yes/no/cancel)? [cancel]:</pre> </li> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Enabling and Configuring Continuity Check for a CFM Service

To configure Continuity Check for a CFM service, complete the following steps:

### SUMMARY STEPS

1. **configure**
2. **ethernet cfm**
3. **domain** *domain-name level level-value* [**id** [null]] [**dns** *DNS-name*] [**mac** *H.H.H*] [**string** *string*]
4. **service** *service-name* {**down-meps** | **xconnect group** *xconnect-group-name p2p xconnect-name*} [**id** [**icc-based** *icc-string umc-string*]] [ [**number** *number*]]
5. **continuity-check interval** *time* [**loss-threshold** *threshold*]
6. **continuity-check archive hold-time** *minutes*
7. **continuity-check loss auto-traceroute**
8. **end** or **commit**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# <code>configure</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ethernet cfm</b> <b>Example:</b> RP/0/RP0/CPU0:router(config)# <code>ethernet cfm</code>	Enters Ethernet Connectivity Fault Management (CFM) configuration mode.
<b>Step 3</b>	<b>domain</b> <i>domain-name level level-value</i> [ <b>id</b> [null]] [ <b>dns</b> <i>DNS-name</i> ] [ <b>mac</b> <i>H.H.H</i> ] [ <b>string</b> <i>string</i> ] <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm)# <code>domain Domain_One level 1 id string D1</code>	Creates and names a container for all domain configurations and enters the CFM domain configuration mode. The level must be specified. The <b>id</b> is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames. If the MDID is not specified, the domain name is used as the MDID by default.
<b>Step 4</b>	<b>service</b> <i>service-name</i> { <b>down-meps</b>   <b>xconnect group</b> <i>xconnect-group-name p2p xconnect-name</i> } [ <b>id</b> [ <b>icc-based</b> <i>icc-string umc-string</i> ]] [ [ <b>number</b> <i>number</i> ]] <b>Example:</b>	Configures and associates a service with the domain and enters CFM domain service configuration mode. You can specify that the service is used only for down MEPs, or associate the service with a xconnect where up MEPs will be created.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config-cfm-dmn)# service xconnect group X1	The <b>id</b> sets the short MA name.
<b>Step 5</b>	<b>continuity-check interval</b> <i>time</i> [ <b>loss-threshold</b> <i>threshold</i> ] <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# continuity-check interval 100m loss-threshold 10	(Optional) Enables Continuity Check and specifies the time interval at which CCMs are transmitted or to set the threshold limit for when a MEP is declared down.
<b>Step 6</b>	<b>continuity-check archive hold-time</b> <i>minutes</i> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# continuity-check archive hold-time 100	(Optional) Configures how long information about peer MEPs is stored after they have timed out.
<b>Step 7</b>	<b>continuity-check loss auto-traceroute</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# continuity-check loss auto-traceroute	(Optional) Configures automatic triggering of a traceroute when a MEP is declared down.
<b>Step 8</b>	<b>end</b> or <b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# commit	Saves configuration changes. <ul style="list-style-type: none"> <li>When you use the <b>end</b> command, the system prompts you to commit changes:  Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</li> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Configuring Cross-Check on a MEP for a CFM Service

To configure cross-check on a MEP for a CFM service and specify the expected set of MEPs, complete the following steps:

## SUMMARY STEPS

1. **configure**
2. **ethernet cfm**
3. **domain** *domain-name level level-value* [**id** [null]] [**dns** *DNS-name*] [**mac** *H.H.H*] [**string** *string*] ]
4. **service** *service-name* {**down-meps** | **xconnect group** *xconnect-group-name p2p xconnect-name*} [**id** [**icc-based** *icc-string umc-string*] | [**string** *text*] | [**number** *number*] | [**vlan-id** *id-number*] | [**vpn-id** *oui-vpnid*]]
5. **mep crosscheck**
6. **mep-id** *mep-id-number* [**mac-address** *mac-address*]
7. **end** or **commit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure</b> <b>Example:</b>  RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	<b>ethernet cfm</b> <b>Example:</b>  RP/0/RP0/CPU0:router# ethernet cfm	Enters the Ethernet Connectivity Fault Management (CFM) configuration mode.
Step 3	<b>domain</b> <i>domain-name level level-value</i> [ <b>id</b> [null]] [ <b>dns</b> <i>DNS-name</i> ] [ <b>mac</b> <i>H.H.H</i> ] [ <b>string</b> <i>string</i> ] ] <b>Example:</b>  RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1	Creates and names a container for all domain configurations and enters the CFM domain configuration mode.  The level must be specified.  The <b>id</b> is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames. If the MDID is not specified, the domain name is used as the MDID by default.
Step 4	<b>service</b> <i>service-name</i> { <b>down-meps</b>   <b>xconnect group</b> <i>xconnect-group-name p2p xconnect-name</i> } [ <b>id</b> [ <b>icc-based</b> <i>icc-string umc-string</i> ]   [ <b>string</b> <i>text</i> ]   [ <b>number</b> <i>number</i> ]   [ <b>vlan-id</b> <i>id-number</i> ]   [ <b>vpn-id</b> <i>oui-vpnid</i> ]]	Configures and associates a service with the domain and enters CFM domain service configuration mode. You can specify that the service is used only for down MEPs, or associate the service with a xconnect where up MEPs will be created.  The <b>id</b> sets the short MA name.
Step 5	<b>mep crosscheck</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# mep crosscheck mep-id 10	Enters CFM MEP crosscheck configuration mode.
Step 6	<b>mep-id</b> <i>mep-id-number</i> [ <b>mac-address</b> <i>mac-address</i> ] <b>Example:</b>	Enables cross-check on a MEP.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config-cfm-xcheck)# mep-id 10	<b>Note</b> <ul style="list-style-type: none"> <li>Repeat this command for every MEP that you want included in the expected set of MEPs for cross-check.</li> </ul>
<b>Step 7</b>	<b>end or commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-xcheck)# commit	Saves configuration changes. <ul style="list-style-type: none"> <li>When you use the <b>end</b> command, the system prompts you to commit changes:   Uncommitted changes found, commit them before exiting (yes/no/cancel)?  [cancel]:</li> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Configuring Other Options for a CFM Service

To configure other options for a CFM service, complete the following steps:

### SUMMARY STEPS

- configure**
- ethernet cfm**
- domain** *domain-name* **level** *level-value* [**id** [null] [**dns** *DNS-name*] [**mac** *H.H.H*] [**string** *string*] ]
- service** *service-name* {**down-meps** | **xconnect group** *xconnect-group-name* **p2p** *xconnect-name*} [**id** [**icc-based** *icc-string umc-string*] | [**string** *text*] | [**number** *number*] | [**vlan-id** *id-number*] | [**vpn-id** *oui-vpnid*]]
- maximum-meps** *number*
- log** {**ais**|**continuity-check errors**|**continuity-check mep changes**|**crosscheck errors**|**efd**}
- end or commit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	<b>ethernet cfm</b> <b>Example:</b> RP/0/RP0/CPU0:router# ethernet cfm	Enters the Ethernet Connectivity Fault Management (CFM) configuration mode.
Step 3	<b>domain domain-name level level-value [id [null] [dns DNS-name] [mac H.H.H] [string string] ]</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1	<p>Creates and names a container for all domain configurations and enters the CFM domain configuration mode.</p> <p>The level must be specified.</p> <p>The <b>id</b> is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames. If the MDID is not specified, the domain name is used as the MDID by default.</p>
Step 4	<b>service service-name {down-meps   xconnect group xconnect-group-name p2p xconnect-name} [id [icc-based icc-string umc-string]   [string text]   [number number]   [vlan-id id-number]   [vpn-id oui-vpnid]]</b>	<p>Configures and associates a service with the domain and enters CFM domain service configuration mode. You can specify that the service is used only for down MEPs, or associate the service with an xconnect where up MEPs will be created.</p> <p>The <b>id</b> sets the short MA name.</p>
Step 5	<b>maximum-meps number</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# maximum-meps 1000	(Optional) Configures the maximum number (2 to 8190) of MEPs across the network, which limits the number of peer MEPs recorded in the database.
Step 6	<b>log {ais continuity-check errors continuity-check mep changes crosscheck errors efd}</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# log continuity-check errors	(Optional) Enables logging of certain types of events.
Step 7	<b>end</b> or <b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# commit	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>When you use the <b>end</b> command, the system prompts you to commit changes:</li> </ul> <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>• Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>• Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Configuring CFM MEPs

- For every subinterface configured under a Layer 3 parent interface, you must associate a unique 802.1Q or 802.1ad tag. Else, it leads to unknown network behavior.

### SUMMARY STEPS

1. **configure**
2. **interface** {**HundredGigE** | **TenGigE**} *interface-path-id*
3. **interface** {**HundredGigE** | **TenGigE** | **Bundle-Ether**} *interface-path-id*2transport
4. **ethernet cfm**
5. **mep domain** *domain-name* **service** *service-name* **mep-id** *id-number*
6. **cos** *cos*
7. **end** or **commit**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> { <b>HundredGigE</b>   <b>TenGigE</b> } <i>interface-path-id</i> <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface TenGigE 0/0/0/1	Type of Ethernet interface on which you want to create a MEP. Enter <b>HundredGigE</b> or <b>TenGigE</b> and the physical interface or virtual interface.



	Command or Action	Purpose
		<p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Use the <b>show interfaces</b> command to see a list of all interfaces currently configured on the router.</li> <li>• L3 interfaces are only supported for bundle member interfaces. Else, you must enable l2transport.</li> </ul>
<b>Step 3</b>	<p><b>interface</b> {<b>HundredGigE</b>   <b>TenGigE</b>   <b>Bundle-Ether</b>} <i>interface-path-id</i>l2transport</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config)# interface TenGigE 0/0/0/1</pre>	<p>Type of Ethernet interface on which you want to create a MEP. Enter <b>HundredGigE</b>, <b>TenGigE</b>, or <b>Bundle-Ether</b> and the physical interface or virtual interface followed by the l2transport. L2transport configures the interface as an L2 interface.</p> <p>Naming convention is <i>interface-path-id.subinterface</i>. The period in front of the subinterface value is required as part of the notation.</p>
<b>Step 4</b>	<p><b>ethernet cfm</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-if)# ethernet cfm</pre>	Enters interface Ethernet CFM configuration mode.
<b>Step 5</b>	<p><b>mep domain</b> <i>domain-name</i> <b>service</b> <i>service-name</i> <b>mep-id</b> <i>id-number</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1</pre>	Creates a maintenance end point (MEP) on an interface and enters interface CFM MEP configuration mode.
<b>Step 6</b>	<p><b>cos</b> <i>cos</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-if-cfm-mep)# cos 7</pre>	<p>(Optional) Configures the class of service (CoS) (from 0 to 7) for all CFM packets generated by the MEP on an interface. If not configured, the CoS is inherited from the Ethernet interface.</p> <p><b>Note</b> For Ethernet interfaces, the CoS is carried as a field in the VLAN tag. Therefore, CoS only applies to interfaces where packets are sent with VLAN tags. If the <b>cos (CFM)</b> command is executed for a MEP on an interface that does not have a VLAN encapsulation configured, it will be ignored.</p>
<b>Step 7</b>	<p><b>end</b> or <b>commit</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-if-cfm-mep)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>• When you use the <b>end</b> command, the system prompts you to commit changes:</li> </ul> <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>• Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>• Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Configuring Y.1731 AIS

This section has the following step procedures:

### Configuring AIS in a CFM Domain Service

Use the following procedure to configure Alarm Indication Signal (AIS) transmission for a CFM domain service and configure AIS logging.

#### SUMMARY STEPS

1. **configure**
2. **ethernet cfm**
3. **domain** *name* **level** *level*
4. **service** *name* **xconnect group** *xconnect-group-name* **p2p** *xconnect-name*
5. **ais transmission** [**interval** {**1s**|**1m**}][**cos** *cos*]
6. **log ais**
7. **end** or **commit**

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>ethernet cfm</b> <b>Example:</b> RP/0/RP0/CPU0:router(config)# ethernet cfm	Enters Ethernet CFM global configuration mode.

	Command or Action	Purpose
Step 3	<p><b>domain</b> <i>name level level</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-cfm)# domain D1 level 1</pre>	Specifies the domain and domain level.
Step 4	<p><b>service</b> <i>name xconnect group xconnect-group-name p2p xconnect-name</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-cfm-dmn)# service S1 xconnect group XG1 p2p X2</pre>	Specifies the service and cross-connect group and name.
Step 5	<p><b>ais transmission</b> [<i>interval {1s 1m}</i>][<i>cos cos</i>]</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# ais transmission interval 1m cos 7</pre>	Configures Alarm Indication Signal (AIS) transmission for a Connectivity Fault Management (CFM) domain service.
Step 6	<p><b>log ais</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-cfm-dmn-svc)# log ais</pre>	Configures AIS logging for a Connectivity Fault Management (CFM) domain service to indicate when AIS or LCK packets are received.
Step 7	<p><b>end</b> or <b>commit</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-sla-prof-stat-cfg)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>When you issue the <b>end</b> command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> </li> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Configuring AIS on a CFM Interface

To configure AIS on a CFM interface, perform the following steps:

### SUMMARY STEPS

1. **configure**
2. **interface gigabitethernet** *interface-path-id*
3. **ethernet cfm**
4. **ais transmission up interval 1m cos** *cos*
5. **end** or **commit**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b>  RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface gigabitethernet</b> <i>interface-path-id</i> <b>Example:</b>  RP/0/RP0/CPU0:router# interface TenGigE 0/0/0/2	Enters interface configuration mode.
<b>Step 3</b>	<b>ethernet cfm</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config)# ethernet cfm	Enters Ethernet CFM interface configuration mode.
<b>Step 4</b>	<b>ais transmission up interval 1m cos</b> <i>cos</i> <b>Example:</b>  RP/0/RP0/CPU0:router(config-if-cfm)# ais transmission up interval 1m cos 7	Configures Alarm Indication Signal (AIS) transmission on a Connectivity Fault Management (CFM) interface.
<b>Step 5</b>	<b>end</b> or <b>commit</b> <b>Example:</b>  RP/0/RP0/CPU0:router(config-sla-prof-stat-cfg)# commit	Saves configuration changes. <ul style="list-style-type: none"> <li>• When you issue the <b>end</b> command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before   exiting(yes/no/cancel)? [cancel]:</pre> </li> <li>• Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>• Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Verifying the CFM Configuration

To verify the CFM configuration, use one or more of the following commands:

<b>show ethernet cfm configuration-errors</b> [domain <i>domain-name</i> ] [interface <i>interface-path-id</i> ]	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.
<b>show ethernet cfm local maintenance-points</b> domain <i>name</i> [service <i>name</i> ]   interface <i>type interface-path-id</i> ] [mep   mip]	Displays a list of local maintenance points.



**Note** After you configure CFM, the error message, *cfmd[317]: %L2-CFM-5-CCM\_ERROR\_CCMS\_MISSED : Some received CCMs have not been counted by the CCM error counters*, may display. This error message does not have any functional impact and does not require any action from you.

## CFM Over Bundles

CFM over bundle supports the following:

- CFM Maintenance Points — UP MEP, Down MEP, which only includes L2 bundle main and sub-interfaces.
- CCM interval of 100 ms, 1s, 10s, 1min, and 10mins.
- RP OIR/VM reload without impacting learnt CFM peer MEPs.
- Process restart without impacting CFM sessions.
- Static MEPs.

### Restrictions for Configuration of CFM on Bundles

Following are the restrictions for configuring CFM over bundle member interfaces:

- Only Layer 2 bundle Ethernet interfaces and sub-interfaces are supported, which are part of a L2VPN cross-connect.
- No support for 3.3ms and 10ms CCM interval.

- Supports 5000 pps rates of CCM traffic for bundle interfaces.
- Ethernet Connectivity Fault Management (CFM) is not supported with Maintenance association End Points (MEPs) that are configured on default and untagged encapsulated sub-interfaces that are part of a single physical interface.
- Multiple MEPs of different directions are not supported on the same interface or Xconnect.

## Ethernet Frame Delay Measurement for L2VPN Services

Table 15: Feature History Table

Feature Name	Release Information	Feature Description
Ethernet Frame Delay Measurement for L2VPN Services	Release 7.5.3	<p>You can now monitor L2VPN networks and avoid impact to your customers' operations by accurately measuring frame round-trip delays and jitters between two maintenance endpoints (MEPs).</p> <p>This feature lets you detect end-to-end connectivity, loopback, and link trace on MEPs. It reports service performance to your end customers, helping improve technical and operational tasks such as troubleshooting and billing.</p> <p>This feature introduces the <b>cfm-delay-measurement probe</b> command.</p>

Ethernet frame delay measurement complies with the ITU-T Y.1731 standard, which provides comprehensive fault management and performance monitoring recommendations. Delay Measurement Message (DMM) and Delay Measurement Reply (DMR) are used to periodically measure one-way or two-way frame delay and frame delay variation between a pair of point-to-point MEPs. Measurements are made between two MEPs belonging to the same domain and Maintenance Association (MA).

You can measure frame delay in the Layer 2 networks to detect end-to-end connectivity, loopback, and link trace on Maintenance End Points (MEPs) and also report service performance that helps to improve technical and operational tasks such as troubleshooting, billing, and so on. Frame delay is the duration between the time the source node transmits the first bit of a frame and the time the same source node receives the last bit of the frame.

The frame delay measurement uses the following two protocol data units (PDUs):

- Delay Measurement Message (DMM)—DMM is used to measure frame delay and frame delay variation between a pair of point-to-point Maintenance End Points (MEPs).
- Delay Measurement Response (DMR)—DMR is the delay measurement response sent by the destination MEP. When an MEP receives a DMM frame, the responder MEP responds with a DMR frame. The DMR frame carries a reply information and a copy of the timestamp contained in the DMM frame.

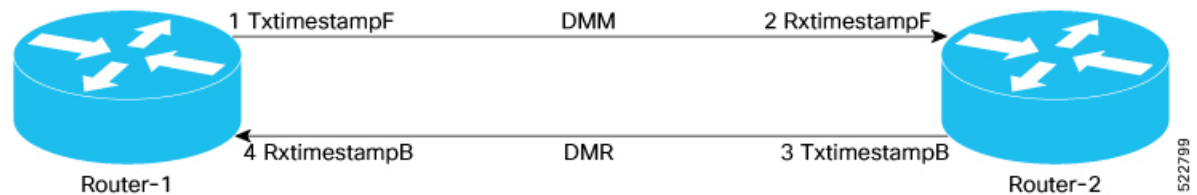
We support one-way and two-way frame delay measurement.

Frame Delay Measurement	Description
One-way frame delay measurement (1DM)	<ul style="list-style-type: none"> <li>Measures the frame delay on a unidirectional link between the MEPs.</li> <li>1DM requires that clocks at both the transmitting MEP and the receiving MEPs are synchronized.</li> <li>Measuring frame-delay variation does not require clock synchronization and the variation can be measured using 1DM and DMR frame combination.</li> </ul>
Two-way frame delay measurement	<ul style="list-style-type: none"> <li>Measures the frame delay on a bidirectional link between the MEPs.</li> <li>Two-way delay measurement does not require the clocks at both the transmitting MEP and the receiving MEPs to be synchronized.</li> <li>The two-way frame delay is measured using only DMM and DMR frames.</li> </ul>

For more information about CFM, see [Configuring Ethernet OAM, on page 55](#).

**Topology**

Let's see how a round-trip frame delay is measured with the following sample topology.



- The sender MEP (Router-1) transmits a frame containing delay measurement request information and the timestamp at the which router sends the DMM.
- When packets pass through each interface, timestamps are written into DMMs and DMRs at both local and peer MEPs.
- When the DMM leaves the local interface, the TX timestamp is added to the packet.
- When the receiver MEP (Router-2) receives the frame, records the timestamp at which the receiver MEP receives the frame with the delay measurement request information and the remote MEP (Router-2) responds with an DMR adding the remote TX timestamp to the packet as it leaves the remote interface.

To measure a round-trip delay for a traffic exchange between Router-1 and Router-2, four timestamps get populated as the packet moves through the network.

- Router-1 adds the TxTimestampF when DMM packet is transmitted.
- Router-2 adds RxTimestampF when DMM packet is received by it.

- Router-2 adds TxTimestampB when DMR packet is transmitted.
- Router-1 adds RxTimestampB when DMR is received by it

The round-trip delay is calculated using the following formula:

$$\begin{aligned} \text{Delay} &= (\text{RxTimestampB} - \text{TxTimestampF}) - (\text{TxTimestampB} - \text{RxTimestampF}) \\ &= \text{RxTimestampB} - \text{TxTimestampF} - \text{TxTimestampB} + \text{RxTimestampF} \\ &= (\text{RxTimestampF} - \text{TxTimestampF}) - (\text{TxTimestampB} - \text{RxTimestampB}) \end{aligned}$$

### Configure Ethernet Frame Delay Measurement for L2VPN Services

Perform the following tasks to configure Ethernet Frame Delay Measurement for L2VPN Services:

1. Configure L2VPN service.
2. Enable CFM service continuity check.
3. Enable CFM on the interface.
4. Configure Ethernet frame delay measurement.

```
/* Configure L2VPN service */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn_vpws_203
Router(config-l2vpn-xc)# p2p evpn_vpws_phy-100
Router(config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/2.100
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 30001 target 30001 source 50001
Router(config-l2vpn-xc-p2p)# commit

/* Enable CFM service continuity check */
Router# ethernet cfm
Router(config-cfm# domain xcupl level 7 id null
Router(config-cfm-dmn)# service xcupl xconnect group evpn_vpws_Bund
Router(config-cfm-dmn-svc)# mip auto-create all ccm-learning
Router(config-cfm-dmn-svc)# continuity-check interval 1s
Router(config-cfm-dmn-svc)# mep crosscheck
Router(config-cfm-dmn-svc)# mep-id 4001
Router(config-cfm-dmn-svc)# commit

/* Enable CFM on the interface */
Router(config)# interface GigabitEthernet0/0/0/2.100 l2transport
Router(config-subif)# encapsulation dot1q 100
Router(config-subif)# rewrite ingress tag pop 1 symmetric
Router(config-subif)# mtu 9100
Router(config-subif)# ethernet cfm
Router(config-if-cfm)# mep domain bd-domain service bd-service mep-id 4001
Router(config-if-cfm-mep)# sla operation profile test-profile1 target mep-id 1112
Router(config-if-cfm-mep)# commit

/* Configure Ethernet frame delay measurement */
Router(config)# ethernet sla
Router(config-sla)# profile EVC-1 type cfm-delay-measurement
Router(config-sla-prof)# probe
Router(config-sla-prof-pb)# send packet every 1 seconds
Router(config-sla-prof-pb)# schedule
Router(config-sla-prof-schedule)# every 3 minutes for 120 seconds
Router(config-sla-prof-schedule)# statistics
Router(config-sla-prof-stat)# measure round-trip-delay
```



```
Router(config-sla-prof-stat-cfg)# buckets size 1 probes
Router(config-sla-prof-stat-cfg)# buckets archive 5
Router(config-sla-prof-stat-cfg)# commit
```

## Running Configuration

This section shows the Ethernet frame delay measurement running configuration.

```
/* Configure L2VPN service */
l2vpn
xconnect group evpn_vpws_203
p2p evpn_vpws_phy-100
interface GigabitEthernet0/0/0/2.100
neighbor evpn evi 30001 target 30001 source 50001
!
/* Enable CFM service continuity check */
ethernet cfm
domain xcup1 level 7 id null
service xcup1 xconnect group evpn_vpws_Bundle_ether203 p2p evpn_vpws-100 id number 4001
mip auto-create all ccm-learning
continuity-check interval 1s
mep crosscheck
mep-id 4001
!
/* Enable CFM on the interface */
interface GigabitEthernet0/0/0/2.100 l2transport
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric
mtu 9100
ethernet cfm
mep domain bd-domain service bd-service mep-id 4001
sla operation profile test-profile1 target mep-id 1112
!
/* Configure Ethernet SLA */
ethernet sla
profile EVC-1 type cfm-delay-measurement
probe
send packet every 1 seconds
!
schedule
every 3 minutes for 120 seconds
!
statistics
measure round-trip-delay
buckets size 1 probes
buckets archive 5
!
```

## Verification

Verify the frame delay measurement. In the following example, you observe that the sent and received DMM and DMR packets are same. So there is no delay in frame transmission.

```
Router# show ethernet cfm local meps interface GigabitEthernet0/0/0/2.100 verbose

Up MEP on GigabitEthernet0/0/0/2.100 MEP-ID 4001
=====
Interface state: Up      MAC address: 0c11.6752.3af8
Peer MEPs: 1 up, 0 with errors, 0 timed out (archived)

CCM generation enabled: Yes, 10s (Remote Defect detected: No)
```

```
AIS generation enabled: No
Sending AIS:             No
Receiving AIS:          No
Sending CSF:            No
Receiving CSF:         No
```

```
Packet      Sent      Received
-----
CCM          19        9 (out of seq: 0)
DMM        473        0
DMR         0         473
```



## CHAPTER 6

# IP Event Dampening

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping.

### Guidelines and Limitations

See the following guidelines and limitations before configuring IP Event Dampening feature:

- Due to changes in the netstack-IP component, all the IP clients observe the impact of dampening or interface.
  - For each flap of the interface, a certain penalty is added. The penalty decays exponentially whose parameters are configured.
  - When penalty exceeds a certain high level, the interface is dampened. It is unsuppressed when the penalty decays below a low level.
  - When an interface is dampened, the IP address and the static routes are removed from the interface. All the clients of IP get an IP delete notification.
  - When an interface is unsuppressed, the IP address and the relevant routes are added back. All the clients of IP get an IP address add notification for all the IP addresses of the interface.
  - All Layer 3 interfaces that are configured on the Ethernet interface, port changes, and SVI support this feature.
- [IP Event Dampening Overview, on page 109](#)
  - [Interface State Change Events, on page 110](#)
  - [Affected Components, on page 111](#)
  - [How to Configure IP Event Dampening, on page 112](#)

## IP Event Dampening Overview

Interface state changes occur when interfaces are administratively brought up or down or if an interface changes state. When an interface changes state or flaps, routing protocols are notified of the status of the routes that are affected by the change in state. Every interface state change requires all affected devices in the network to recalculate best paths, install or remove routes from the routing tables, and then advertise valid routes to peer routers. An unstable interface that flaps excessively can cause other devices in the network to

consume substantial amounts of system processing resources and cause routing protocols to lose synchronisation with the state of the flapping interface.

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping. Dampening an interface removes the interface from the network until the interface stops flapping and becomes stable. Configuring the IP Event Dampening feature improves convergence times and stability throughout the network by isolating failures so that disturbances are not propagated. This, in turn, reduces the utilisation of system processing resources by other devices in the network and improves overall network stability.

## Interface State Change Events

This section describes the interface state change events of the IP Event Dampening feature. This feature employs a configurable exponential decay mechanism that is used to suppress the effects of excessive interface flapping or state changes. When the IP Event Dampening feature is enabled, flapping interfaces are dampened from the perspective of the routing protocol by filtering excessive route updates. Flapping interfaces are identified, assigned penalties, suppressed if necessary, and made available to the network when the interface stabilizes.

### Suppress Threshold

The suppress threshold is the value of the accumulated penalty that triggers the router to dampen a flapping interface. The flapping interface is identified by the router and assigned a penalty for each up and down state change, but the interface is not automatically dampened. The router tracks the penalties that a flapping interface accumulates. When the accumulated penalty reaches the default or preconfigured suppress threshold, the interface is placed in a dampened state.

### Half-Life Period

The half-life period determines how fast the accumulated penalty can decay exponentially. When an interface is placed in a dampened state, the router monitors the interface for additional up and down state changes. If the interface continues to accumulate penalties and the interface remains in the suppress threshold range, the interface will remain dampened. If the interface stabilises and stops flapping, the penalty is reduced by half after each half-life period expires. The accumulated penalty will be reduced until the penalty drops to the reuse threshold. The configurable range of the half-life period timer is from 1 to 45 minutes. The default half-life period timer is 1 minute.

### Reuse Threshold

When the accumulated penalty decreases until the penalty drops to the reuse threshold, the route is unsuppressed and made available to other devices in the network. The range of the reuse value is from 1 to 20000 penalties. The default value is 750 penalties.

## Maximum Suppress Time

The maximum suppress time represents the maximum time an interface can remain dampened when a penalty is assigned to an interface. The maximum suppress time can be configured from 1 to 255 seconds. The maximum penalty is truncated to maximum 20000 unit. The maximum value of the accumulated penalty is calculated based on the maximum suppress time, reuse threshold, and half-life period.

## Affected Components

When an interface is not configured with dampening, or when an interface is configured with dampening but is not suppressed, the routing protocol behavior as a result of interface state transitions is not changed by the IP Event Dampening feature. However, if an interface is suppressed, the routing protocols and routing tables are immune to any further state transitions of the interface until it is unsuppressed.

## Route Types

The following interfaces are affected by the configuration of this feature:

- Connected routes:
  - The connected routes of dampened interfaces are not installed into the routing table.
  - When a dampened interface is unsuppressed, the connected routes will be installed into the routing table if the interface is up.
- Static routes:
  - Static routes assigned to a dampened interface are not installed into the routing table.
  - When a dampened interface is unsuppressed, the static route will be installed into the routing table if the interface is up.



---

**Note** Only the primary interface can be configured with this feature, and all subinterfaces are subject to the same dampening configuration as the primary interface. IP Event Dampening does not track the flapping of individual subinterfaces on an interface.

---

## Supported Protocols

All the protocols that are used are impacted by the IP Event Dampening feature. The IP Event Dampening feature supports Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Hot Standby Routing Protocol (HSRP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and VRRP. Ping and SSH to the concerned interface IP address does not work.



---

**Note** The IP Event Dampening feature has no effect on any routing protocols if it is not enabled or an interface is not dampened.

---

# How to Configure IP Event Dampening

## Enabling IP Event Dampening

The `dampening` command is entered in interface configuration mode to enable the IP Event Dampening feature. If this command is applied to an interface that already has dampening configured, all dampening states are reset and the accumulated penalty will be set to 0. If the interface has been dampened, the accumulated penalty will fall into the reuse threshold range, and the dampened interface will be made available to the network. The flap counts, however, are retained.

**Table 16: Procedure**

Steps	Command or Action	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>interface</b> <i>type number</i>	Enters interface configuration mode and configures the specified interface.
Step 3	<b>dampening</b> [ <i>half-life-period reuse-threshold</i> ] [ <i>suppress-threshold max-suppress [restart-penalty]</i> ]	Enables interface dampening. <ul style="list-style-type: none"> <li>• Entering the <code>dampening</code> command without any arguments enables interface dampening with default configuration parameters.</li> <li>• When manually configuring the timer for the <code>restart-penalty</code> argument, the values must be manually entered for all arguments.</li> </ul>
Step 4	<b>end</b>	Exits interface configuration mode.

## Verifying IP Event Dampening

Use the `show dampening interface` or `show interface dampening` commands to verify the configuration of the IP Event Dampening feature.

**Table 17: Procedure**

Steps	Command or Action	Purpose
Step 1	<b>show dampening interface</b>	Displays dampened interfaces.
Step 2	<b>show interface dampening</b>	Displays dampened interfaces on the local router.



# CHAPTER 7

## Configuring Link Bundling

Table 18: Feature History Table

Feature Name	Release	Description
1023 Ethernet Bundle Interfaces Support	Release 7.3.15	With the introduction of this enhancement, the maximum system-wide bundle interface scale has increased from 512 to 1023 bundle interfaces. The default value remains at 64-member links for each bundle.
64-bit Bandwidth Support	Release 7.3.15	With this release, the Cisco 8000 Series Router supports 64-bit bandwidth field, as opposed to the previous 32-bit bandwidth field. 64-bit bandwidth enables the system to support interface bandwidths greater than 4.2T.

This module describes the configuration of link bundle interfaces on the Cisco 8000 Series Router.

A link bundle is a group of one or more ports that are aggregated together and treated as a single link.

Each bundle has a single MAC, a single IP address, and a single configuration set (such as ACLs).



**Note** The router supports both Layer 2 and Layer 3 Link Bundles. If the Link Bundle is a Layer 3 interface, the system requires an IP address. If the Link Bundle is a Layer 2 interface, the system does not require an IP address. A Link Bundle on the router may contain Layer 2 and Layer 3 subinterfaces within it. In which case, the Layer 3 subinterfaces require IP addresses, but the Link Bundle interface does not require an IP address.

The router supports bundling for these types of interfaces:

- Ethernet interfaces

### Feature History for Configuring Link Bundling

Release	Modification
Release 7.0.11	Support for this feature added on the router.

Release 7.2.1	Mixed speed bundle members feature added on the router.
---------------	---

- [Limitations and Compatible Characteristics of Ethernet Link Bundles, on page 114](#)
- [Prerequisites for Configuring Link Bundling on a Router, on page 115](#)
- [Information About Configuring Link Bundling, on page 116](#)
- [How to Configure Link Bundling, on page 128](#)
- [Configuration Examples for Link Bundling, on page 136](#)

## Limitations and Compatible Characteristics of Ethernet Link Bundles

This list describes the properties and limitations of ethernet link bundles:

- The router supports mixed speed bundles. Mixed speed bundles allow member links of different bandwidth to be configured as active members in a single bundle. The ratio of the bandwidth for bundle members must not exceed 10. Also, the total weight of the bundle must not exceed 64. For example, 100Gbps link and 10Gbps links can be active members in a bundle and load-balancing on member links are based on bandwidth weightage.
- Starting with Cisco IOS XR Release 7.2.1, the router supports mixed speed bundle members in a bundle. Traffic flows are distributed based on the bandwidth of each member link. Mixed speed combinations support a maximum ratio of 10:1. For example, a 10Gbps and a 100Gbps link can be mixed, or a 100Gbps and a 400Gbps link can be mixed, but a 10Gbps and a 400Gbps link cannot be mixed. The following combinations are possible:
  - 400G, 100G
  - 400G, 40G
  - 400G, 100G, 40G
  - 100G, 40G
  - 100G, 10G
  - 100G, 40G, 10G
  - 40G and 10G
- The weight of each bundle member is the ratio of its bandwidth to the lowest bandwidth member. Total weight of the bundle is the sum of weights or relative bandwidth of each bundle member. Since the weight for a bundle member is greater than or equal to 1 and less than or equal to 10, the total member of links in a bundle is less than 64 in mixed bundle case.
- Any type of Ethernet interfaces can be bundled, with or without the use of LACP (Link Aggregation Control Protocol).
- A single router can support a maximum of 512 bundle interfaces and a default of 64 member links per bundle.
- A single router supports up to a maximum of 2000 bundle subinterfaces.



- With Cisco IOS XR Release 7.3.15, a single router supports up to a maximum of 1023 bundle interfaces and up to a maximum of 64 member links per bundle.

The total number of L3 interfaces and bundle members on the system must not exceed 2047. This limitation means that you can have 1023 bundle with one member each (1023 bundle member) and a single physical interface in the system. When you initialise the line cards, the system applies the 2047 limit automatically.

Any newly inserted line card, which leads to exceeding this scale encounters continuous Out of Resource (OOR) failures. To stop the errors, reduce the scale or shut the line card.

- Physical layer and link layer configuration are performed on individual member links of a bundle.
- Configuration of network layer protocols and higher layer applications is performed on the bundle itself.
- IPv4 and IPv6 addressing is supported on ethernet link bundles.
- A bundle can be administratively enabled or disabled.
- Each individual link within a bundle can be administratively enabled or disabled.
- Ethernet link bundles are created in the same way as Ethernet channels, where the user enters the same configuration on both end systems.
- The MAC address that is set on the bundle becomes the MAC address of the links within that bundle.
- Load balancing (the distribution of data between member links) is done by flow instead of by packet. Data is distributed to a link in proportion to the bandwidth of the link in relation to its bundle.
- QoS is supported and is applied proportionally on each bundle member.
- All links within a single bundle must terminate on the same two systems.
- Bundled interfaces are point-to-point.
- A link must be in the up state before it can be in distributing state in a bundle.
- Only physical links can be bundle members.

## Prerequisites for Configuring Link Bundling on a Router

Before configuring Link Bundling, ensure that you meet the following tasks and conditions:

- You know the interface IP address (Layer 3 only).
- You know the links that you must include in the bundle that you are configuring.
- If you are configuring an Ethernet link bundle, you must install Ethernet line cards on the router.



---

**Note** For more information about physical interfaces, PLIMs, and modular services cards, refer to the *Cisco 8000 Series Router Hardware Installation Guide*.

---

# Information About Configuring Link Bundling

To configure link bundling, you must understand the following concepts:

## Link Bundling Overview

The Link Bundling feature allows you to group multiple point-to-point links together into one logical link and provide higher bidirectional bandwidth, redundancy, and load balancing between two routers. The system assigns a virtual interface to the bundled link. You can dynamically add and delete component links from the virtual interface.

The virtual interface is treated as a single interface on which you can configure an IP address and other software features that the link bundle uses. Packets sent to the link bundle are forwarded to one of the links in the bundle.

A link bundle is a group of ports that the system bundles together and the group then acts as a single link. Following are the advantages of link bundles:



---

**Note** A single router supports 512 bundles per system.

---

- Multiple links can span several line cards to form a single interface. Thus, the failure of a single link does not cause a loss of connectivity.
- Bundled interfaces increase bandwidth availability, because traffic is forwarded over all available members of the bundle. Therefore, traffic can flow on the available links, if one of the links within a bundle fails. You can add bandwidth without interrupting the packet flow.

The previous Cisco IOS XR Software Releases stored and processed the interface bandwidth as a 32-bit value, which supported bundles with an aggregate bandwidth (from the sum of its members) up to 4.2 Gbps. With Cisco IOS XR Software Release 7.3.15, the interface bandwidth is stored and processed as a 64-bit value. The 64-bit value supports larger aggregate bandwidth as some bundles now contain sufficient high bandwidth members that the aggregate value can exceed the 4.2 Gbps bandwidth.

All the individual links within a single bundle must be of the same type.

Cisco IOS XR software supports the following methods of forming bundles of Ethernet interfaces:

- IEEE 802.3ad—Standard technology that employs a Link Aggregation Control Protocol (LACP) to ensure that all the member links in a bundle are compatible. The system automatically removes the links from a bundle that are incompatible or have failed.

## Link Aggregation Through LACP

The optional Link Aggregation Control Protocol (LACP) is defined in the IEEE 802 standard. LACP communicates between two directly connected systems (or peers) to verify the compatibility of bundle members. For the router, the peer can be either another router or a switch. LACP monitors the operational state of link bundles to ensure the following:

- All links terminate on the same two systems.

- Both systems consider the links to be part of the same bundle.
- All links have the appropriate settings on the peer.

LACP transmits frames containing the local port state and the local view of the partner system's state. The system analyzes these frames to ensure that both the systems are in agreement.

## IEEE 802.3ad Standard

The IEEE 802.3ad standard typically defines a method of forming Ethernet link bundles.

For each link configured as a bundle member, the following information is exchanged between the systems that host each end of the link bundle:

- A globally unique local system identifier.
- An identifier (operational key) for the bundle of which the link is a member.
- An identifier (port ID) for the link.
- The current aggregation status of the link.

This information is used to form the link aggregation group identifier (LAG ID). Links that share a common LAG ID can be aggregated. Individual links have unique LAG IDs.

The system identifier distinguishes one router from another, and its uniqueness is guaranteed by using a MAC address from the system. The bundle and link identifiers have significance only to the router assigning them, which must guarantee that no two links have the same identifier, and that no two bundles have the same identifier.

The information from the peer system is combined with the information from the local system. This determines the compatibility of the links that are configured to be members of a bundle.

Bundle MAC addresses in the router come from a set of reserved MAC addresses in the backplane. This MAC address stays with the bundle as long as the bundle interface exists. The bundle uses this MAC address until you configure a different MAC address. The member links use the bundle MAC address when passing the bundle traffic. Any unicast or multicast addresses set on the bundle are also set on all the member links.



---

**Note** We recommend that you avoid modifying the MAC address, because changes in the MAC address can affect packet forwarding.

---

## Configuring LACP Fallback

This section describes how to configure the LACP Fallback feature.

---

### Step 1 **configure**

#### **Example:**

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

Enters global configuration mode.

**Step 2** `interface Bundle-Ether bundle-id`**Example:**

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 3
```

Creates and names a new Ethernet link bundle.

This **interface Bundle-Ether** command enters you into the interface configuration submode, where you can enter interface-specific configuration commands. Use the **exit** command to exit from the interface configuration submode back to the normal global configuration mode.

**Step 3** `ipv4 address ipv4-address mask`**Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle lacp-fallback timeout 4
```

Enables the LACP Fallback feature.

**Step 4** `end` or `commit`**Example:**

```
RP/0/RP0/CPU0:router(config-subif)# commit
```

Saves configuration changes.

**Step 5** `show bundle infrastructure database ma bdl-info Bundle-e1010 | inctext`**Example:**

```
RP/0/RP0/CPU0:router# show bundle infrastructure database ma bdl-info Bundle-e1010 | inc "fallback"
```

(Optional) Shows the MA information of the bundle manager.

**Step 6** `show bundle infrastructure database ma bdl-info Bundle-e1015 | inctext`**Example:**

```
RP/0/RP0/CPU0:router# show bundle infrastructure database ma bdl-info Bundle-e1015 | inc "fallback"
```

(Optional) Shows the MA information of the bundle manager.

---

## LACP Short Period Time Intervals

As packets are exchanged across member links of a bundled interface, some member links may slow down or time-out and fail. LACP packets are exchanged periodically across these links to verify the stability and reliability of the links over which they pass. The configuration of short period time intervals, in which LACP packets are sent, enables faster detection and recovery from link failures.

Short period time intervals are configured as follows:

- In milliseconds
- In increments of 100 milliseconds
- In the range 100 to 1000 milliseconds

- The default is 1000 milliseconds (1 second)
- Up to 64 member links
- Up to 1280 packets per second (pps)

After 6 missed packets, the link is detached from the bundle.

When the short period time interval is *not* configured, LACP packets are transmitted over a member link every 30 seconds by default.

When the short period time interval is configured, LACP packets are transmitted over a member link once every 1000 milliseconds (1 second) by default. Optionally, both the transmit and receive intervals can be configured to less than 1000 milliseconds, independently or together, in increments of 100 milliseconds (100, 200, 300, and so on).

When you configure a custom LACP short period *transmit* interval at one end of a link, you must configure the same time period for the *receive* interval at the other end of the link.



---

**Note** You must always configure the *transmit* interval at both ends of the connection before you configure the *receive* interval at either end of the connection. Failure to configure the *transmit* interval at both ends first results in route flapping (a route going up and down continuously). When you remove a custom LACP short period, you must do it in reverse order. You must remove the *receive* intervals first and then the *transmit* intervals.

---

## Load Balancing

Load balancing is a forwarding mechanism that distributes traffic over multiple links that are based on certain parameters. The router support load balancing for all links in a bundle using Layer 2, Layer 3, and Layer 4 routing information. Starting with Cisco IOS XR Software Release 7.2.1, bandwidth based load-balancing is applicable to L3 unicast flows.

This section describes the load balancing support on link bundles.

For more information about other forms of load balancing on the router, see the following:

- Per-flow load balancing on non-bundle interfaces using Layer 3 and 4 routing information.
- Pseudowire (PW) Load Balancing beginning in Cisco IOS XR 4.0.1.

## Layer 3 Egress Load Balancing on Link Bundles

Layer 3 load balancing support began on the router in Cisco IOS XR 7.0.11 release.

Layer 3 load balancing for link bundles is enabled globally by default.

The ingress linecard does bundle member selection and forwards the packet to the linecard and network processor (NP) corresponding to the selected bundle member. The same hash value is used for both ingress and egress linecards. Therefore, even though the egress linecard also does bundle member selection, it selects the same bundle member that was selected by the ingress linecard.

### Multicast IPv4 and IPv6 Traffic

For outbound multicast IPv4 or IPv6 traffic, a set of egress linecards is predetermined by the system. If a bundle interface or bundle subinterface is an outgoing interface, the system selects the bundle member for each outgoing interface in a route based on the multicast group address. This helps with load distribution of multicast routed traffic to different bundle members, while providing traffic sequencing within a specific route.

The egress linecard does NP selection using the same approach, when bundle members are spread across multiple NPs within the egress linecard.

When the packet arrives on an egress NP, it uses the 5-tuple hash to select a bundle member within an NP for each packet. This provides better resiliency for bundle member state changes within an NP.

## Configuring the Default LACP Short Period Time Interval

This section describes how to configure the default short period time interval for sending and receiving LACP packets on a Gigabit Ethernet interface. This procedure also enables the LACP short period.

### Step 1 **configure**

#### Example:

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

Enters global configuration mode.

### Step 2 **interface HundredGigE***interface-path*

#### Example:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/1/0/1
```

Creates a Gigabit Ethernet interface and enters interface configuration mode.

### Step 3 **bundle id** *number* **mode active**

#### Example:

```
RP/0/RP0/CPU0:router(config-if)# bundle id 1 mode active
```

Specifies the bundle interface and puts the member interface in active mode.

### Step 4 **lacp period short**

#### Example:

```
RP/0/RP0/CPU0:router(config-if)# lacp period short
```

Configures a short period time interval for the sending and receiving of LACP packets, using the default time period of 1000 milliseconds or 1 second.

### Step 5 **end** or **commit**

#### Example:

```
RP/0/RP0/CPU0:router(config-if)# end
```

or

```
RP/0/RP0/CPU0:router(config-if)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before
exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

---

### Example

This example shows how to configure the LACP short period time interval to the default time of 1000 milliseconds (1 second):

```
config
interface HundredGigE 0/1/0/1
  bundle id 1 mode active
  lacp period short
  commit
```

The following example shows how to configure custom LACP short period transmit and receive intervals to *less than* the default of 1000 milliseconds (1 second):

```
config
interface HundredGigE 0/1/0/1
  bundle id 1 mode active
  lacp period short
  commit

config
interface HundredGigE 0/1/0/1
  lacp period short transmit 100
  commit

config
interface HundredGigE 0/1/0/1
  lacp period short receive 100
  commit
```

## Configuring Custom LACP Short Period Time Intervals

**Step 1** `interface Bundle-Ether bundle-id`

**Example:**

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 3
```

Creates and names a new Ethernet link bundle.

This **interface Bundle-Ether** command enters you into the interface configuration submode, where you can enter interface-specific configuration commands. Use the **exit** command to exit from the interface configuration submode back to the normal global configuration mode.

**Step 2** `ipv4 address ipv4-address mask`

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.2.3 255.0.0.0
```

Assigns an IP address and subnet mask to the virtual interface using the **ipv4 address** configuration subcommand.

**Step 3** `bundle minimum-active bandwidth kbps`

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle minimum-active bandwidth 580000
```

(Optional) Sets the minimum amount of bandwidth required before a user can bring up a bundle.

**Step 4** `bundle minimum-active links links`

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle minimum-active links 2
```

(Optional) Sets the number of active links required before you can bring up a specific bundle.

**Step 5** `bundle maximum-active links links`

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle maximum-active links 1
```

(Optional) Designates one active link and one link in standby mode that can take over immediately for a bundle if the active link fails (1:1 protection).

**Note**

- The default number of active links allowed in a single bundle is 8.
- If the **bundle maximum-active** command is issued, then only the highest-priority link within the bundle is active. The priority is based on the value from the **bundle port-priority** command, where a lower value is a higher priority. Therefore, we recommend that you configure a higher priority on the link that you want to be the active link.

**Step 6** `exit`

**Example:**



```
RP/0/RP0/CPU0:router(config-if)# exit
```

Exits the interface configuration submode.

**Step 7**      **interface Bundle-Ether** *bundle-id.vlan-id*

**Example:**

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether 3.1
```

Creates a new VLAN, and assigns the VLAN to the Ethernet bundle you created in Step 2.

Replace the *bundle-id* argument with the *bundle-id* you created in Step 2.

Replace the *vlan-id* with a subinterface identifier. Range is from 1 to 4094 inclusive (0 and 4095 are reserved).

**Note**              • When you include the *.vlan-id* argument with the **interface Bundle-Ether** *bundle-id* command, you enter subinterface configuration mode.

**Step 8**      **dot1q vlan** *vlan-id*

**Example:**

```
RP/0/RP0/CPU0:router(config-subif)# dot1q vlan 10
```

Assigns a VLAN to the subinterface.

Replace the *vlan-id* argument with a subinterface identifier. Range is from 1 to 4094 inclusive (0 and 4095 are reserved).

**Step 9**      **ipv4 address** *ipv4-address mask*

**Example:**

```
RP/0/RP0/CPU0:router#(config-subif)# ipv4 address 10.1.2.3/24
```

Assigns an IP address and subnet mask to the subinterface.

**Step 10**     **no shutdown**

**Example:**

```
RP/0/RP0/CPU0:router(config-subif)# no shutdown
```

(Optional) If a link is in the down state, bring it up. The **no shutdown** command returns the link to an up or down state depending on the configuration and state of the link.

**Step 11**     **exit**

**Example:**

```
RP/0/RP0/CPU0:router(config-subif)# exit
```

Exits subinterface configuration mode for the VLAN subinterface.

**Step 12**     Repeat Step 7 through Step 12 to add more VLANs to the bundle you created in Step 2.

(Optional) Adds more subinterfaces to the bundle.

**Step 13**     **end** or **commit**

**Example:**

```
RP/0/RP0/CPU0:router(config-subif)# end
```

or

```
RP/0/RP0/CPU0:router(config-subif)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)?
- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

**Step 14**    **exit****Example:**

```
RP/0/RP0/CPU0:router(config-subif)# exit
```

Exits interface configuration mode.

**Step 15**    **exit****Example:**

```
RP/0/RSP0/CPU0:router(config)# exit
```

Exits global configuration mode.

**Step 16**    **show ethernet trunk bundle-ether** *instance***Example:**

```
RP/0/RP0/CPU0:router# show ethernet trunk bundle-ether 5
```

(Optional) Displays the interface configuration.

The Ethernet bundle instance range is from 1 through 65535.

**Step 17**    **configure****Example:**

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

Enters global configuration mode.

**Step 18**    **interface** {GigabitEthernet | TenGigE} *interface-path-id*

**Example:**

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 1/0/0/0
```

Enters the interface configuration mode for the Ethernet interface you want to add to the Bundle.

Enter the **GigabitEthernet** or **TenGigE** keyword to specify the interface type. Replace the *interface-path-id* argument with the node-id in the rack/slot/module format.

**Note** • A VLAN bundle is not active until you add an Ethernet interface on both ends of the link bundle.

**Step 19** **bundle id** *bundle-id* [**mode** {**active** | **on** | **passive**}]**Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle-id 3
```

Adds an Ethernet interface to the bundle you configured in Step 2 through Step 13.

To enable active or passive LACP on the bundle, include the optional **mode active** or **mode passive** keywords in the command string.

To add the interface to the bundle without LACP support, include the optional **mode on** keywords with the command string.

**Note** • If you do not specify the **mode** keyword, the default mode is **on** (LACP is not run over the port).

**Step 20** **no shutdown****Example:**

```
RP/0/RP0/CPU0:router(config-if)# no shutdown
```

(Optional) If a link is in the down state, bring it up. The **no shutdown** command returns the link to an up or down state depending on the configuration and state of the link.

**Step 21** Repeat Step 19 through Step 21 to add more Ethernet interfaces to the VLAN bundle.

—

**Step 22** **end** or **commit****Example:**

```
RP/0/RP0/CPU0:router(config-subif)# end
```

or

```
RP/0/RP0/CPU0:router(config-subif)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)?
- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

**Step 23** Perform Step 1 through Step 23 on the remote end of the VLAN bundle connection.

Brings up the other end of the link bundle.

**Step 24** **show bundle Bundle-Ether** *bundle-id* [**reasons**]

**Example:**

```
RP/0/RP0/CPU0:router# show bundle Bundle-Ether 3 reasons
```

(Optional) Shows information about the specified Ethernet link bundle.

The **show bundle Bundle-Ether** command displays information about the specified bundle. If your bundle has been configured properly and is carrying traffic, the State field in the **show bundle Bundle-Ether** command output will show the number “4,” which means the specified VLAN bundle port is “distributing.”

**Step 25** **show ethernet trunk bundle-ether** *instance*

**Example:**

```
RP/0/RP0/CPU0:router# show ethernet trunk bundle-ether 5
```

(Optional) Displays the interface configuration.

The Ethernet bundle instance range is from 1 through 65535.

## QoS and Link Bundling

On the router, when the system applies QoS on the bundle for either the ingress or egress direction, QoS is applied at each member interface. For complete information on configuring QoS on link bundles on the router, refer to the *Cisco 8000 Series Aggregation Services Router Modular Quality of Service Configuration Guide* and the *Cisco 8000 Series Aggregation Services Router Modular Quality of Service Command Reference*.

## Link Bundle Configuration Overview

The following steps provide a general overview of the link bundle configuration process. Ensure that you clear all previous network layer configuration before adding it to a bundle:

1. In global configuration mode, create a link bundle. To create an Ethernet link bundle, enter the **interface Bundle-Ether** command.
2. Assign an IP address and subnet mask to the virtual interface using the **ipv4 address** command.
3. Add interfaces to the bundle that you created in Step 1 with the **bundle id** command in the interface configuration submode.

You can add up to 64 links to a single bundle.



---

**Note** The system configures a link as a member of a bundle from the interface configuration submode for that link.

---

## Nonstop Forwarding During Card Failover

Cisco IOS XR software supports nonstop forwarding during a failover between active and standby paired RP cards. Nonstop forwarding ensures that there is no change in the state of the link bundles when a failover occurs.

For example, if an active RP fails, the standby RP becomes operational. The system replicates the configuration, node state, and checkpoint data of the failed RP to the standby RP. The bundled interfaces are present when the standby RP becomes the active RP.



---

**Note** Failover is always onto the standby RP.

You do not need to configure anything to guarantee that the system maintains the standby interface configurations.

---

## Link Failover

When one member link in a bundle fails, the system redirects the to the remaining operational member links and traffic flow remains uninterrupted.

## Link Switchover

By default, a maximum of 64 links in a bundle can actively carry traffic. If one member link in a bundle fails, traffic is redirected to the remaining operational member links.

You can optionally implement 1:1 link protection for a bundle by setting the **bundle maximum-active links** command to 1. By doing so, you designate one active link and one or more dedicated standby links. If the active link fails, a switchover occurs and a standby link immediately becomes active, thereby ensuring uninterrupted traffic.

If the active and standby links are running LACP, you can choose between an IEEE standard-based switchover (the default) or a faster proprietary optimized switchover. If the active and standby links are not running LACP, the proprietary optimized switchover option is used.

Regardless of the type of switchover you are using, you can disable the wait-while timer, which expedites the state negotiations of the standby link and causes a faster switchover from a failed active link to the standby link.

To do so, you can use the **lACP switchover suppress-flaps** command.

## LACP Fallback

The LACP Fallback feature allows an active LACP interface to establish a Link Aggregation Group (LAG) port-channel before the port-channel receives the Link Aggregation and Control Protocol (LACP) protocol data units (PDU) from its peer.

With the LACP Fallback feature configured, the router allows the server to bring up the LAG, before receiving any LACP PDUs from the server, and keeps one port active. This allows the server to establish a connection to PXE server over one Ethernet port, download its boot image and then continue the booting process. When the server boot process is complete, the server fully forms an LACP port-channel.

## How to Configure Link Bundling

This section contains the following procedures:

### Configuring Ethernet Link Bundles

This section describes how to configure an Ethernet link bundle.



**Note** In order for an Ethernet bundle to be active, you must perform the same configuration on both connection endpoints of the bundle.



**Tip** You can programmatically perform the configuration using `openconfig-lacp.yang`, `openconfig-if-aggregate.yang` OpenConfig data models, `Cisco-IOS-XR-bundlemgr-oper.yang` Cisco IOS XR native data model or `Cisco-IOS-XR-um-lacp-cfg.yang` Unified data model. To get started with using data models, see the *Programmability Configuration Guide for Cisco 8000 Series Routers*.

#### Step 1 **configure**

##### **Example:**

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

Enters global configuration mode.

#### Step 2 **interface Bundle-Ether *bundle-id***

##### **Example:**

```
RP/0/RP0/CPU0:router#(config)# interface Bundle-Ether 3
```

Creates a new Ethernet link bundle with the specified bundle-id. The range is 1 to 65535.

This **interface Bundle-Ether** command enters you into the interface configuration submode, where you can enter interface specific configuration commands are entered. Use the **exit** command to exit from the interface configuration submode back to the normal global configuration mode.

**Step 3**      **ipv4 address** *ipv4-address mask***Example:**

```
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.2.3 255.0.0.0
```

Assigns an IP address and subnet mask to the virtual interface using the **ipv4 address** configuration subcommand.

**Note**            • On the router, only a Layer 3 bundle interface requires an IP address.

**Step 4**      **bundle minimum-active bandwidth** *kbps***Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle minimum-active bandwidth 580000
```

(Optional) Sets the minimum amount of bandwidth required before a user can bring up a bundle.

**Step 5**      **bundle minimum-active links** *links***Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle minimum-active links 2
```

(Optional) Sets the number of active links required before you can bring up a specific bundle.

**Step 6**      **bundle maximum-active links** *links* [**hot-standby**]**Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle maximum-active links 1 hot-standby
```

(Optional) Implements 1:1 link protection for the bundle, which causes the highest-priority link in the bundle to become active and the second-highest-priority link to become the standby. Also, specifies that a switchover between active and standby LACP-enabled links is implemented per a proprietary optimization.

**Note**            • The priority of the active and standby links is based on the value of the **bundle port-priority** command.

**Step 7**      **lACP fast-switchover****Example:**

```
RP/0/RP0/CPU0:router(config-if)# lACP fast-switchover
```

(Optional) If you enabled 1:1 link protection (you set the value of the **bundle maximum-active links** command to 1) on a bundle with member links running LACP, you can optionally disable the wait-while timer in the LACP state machine. Disabling this timer causes a bundle member link in standby mode to expedite its normal state negotiations, thereby enabling a faster switchover from a failed active link to the standby link.

**Step 8**      **exit****Example:**

```
RP/0/RP0/CPU0:router(config-if)# exit
```

Exits interface configuration submode for the Ethernet link bundle.

**Step 9**      **interface** {**GigabitEthernet** | **TenGigE**} *interface-path-id*

**Example:**

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 1/0/0/0
```

Enters interface configuration mode for the specified interface.

Enter the **GigabitEthernet** or **TenGigE** keyword to specify the interface type. Replace the *interface-path-id* argument with the node-id in the *rack/slot/module* format.

**Step 10** **bundle id** *bundle-id* [**mode** {**active** | **on** | **passive**}]**Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle-id 3
```

Adds the link to the specified bundle.

To enable active or passive LACP on the bundle, include the optional **mode active** or **mode passive** keywords in the command string.

To add the link to the bundle without LACP support, include the optional **mode on** keywords with the command string.

**Note** • If you do not specify the **mode** keyword, the default mode is **on** (LACP is not run over the port).

**Step 11** **bundle port-priority** *priority***Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle port-priority 1
```

(Optional) If you set the **bundle maximum-active links** command to 1, you must also set the priority of the active link to the highest priority (lowest value) and the standby link to the second-highest priority (next lowest value). For example, you can set the priority of the active link to 1 and the standby link to 2.

**Step 12** **no shutdown****Example:**

```
RP/0/RP0/CPU0:router(config-if)# no shutdown
```

(Optional) If a link is in the down state, bring it up. The **no shutdown** command returns the link to an up or down state depending on the configuration and state of the link.

**Step 13** **exit****Example:**

```
RP/0/RP0/CPU0:router(config-if)# exit
```

Exits interface configuration submode for the Ethernet interface.

**Step 14** **bundle id** *bundle-id* [**mode** {**active** | **passive** | **on**}] **no shutdown exit****Example:**

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 1/0/2/1
```

```
RP/0/RP0/CPU0:router(config-if)# bundle id 3
```



```
RP/0/RP0/CPU0:router(config-if)# bundle port-priority 2
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# exit
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 1/0/2/3
RP/0/RP0/CPU0:router(config-if)# bundle id 3
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# exit
```

(Optional) Repeat Step 8 through Step 11 to add more links to the bundle.

### Step 15 **end** or **commit**

#### **Example:**

```
RP/0/RP0/CPU0:router(config-if)# end
or
RP/0/RP0/CPU0:router(config-if)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

### Step 16 **exit**

#### **Example:**

```
RP/0/RP0/CPU0:router(config-if)# exit
Exits interface configuration mode.
```

### Step 17 **exit**

#### **Example:**

```
RP/0/RP0/CPU0:router(config)# exit
Exits global configuration mode.
```

**Step 18** Perform Step 1 through Step 15 on the remote end of the connection.  
Brings up the other end of the link bundle.

**Step 19** **show bundle Bundle-Ether** *bundle-id*

**Example:**

```
RP/0/RP0/CPU0:router# show bundle Bundle-Ether 3
```

(Optional) Shows information about the specified Ethernet link bundle.

**Step 20** **show lacp bundle Bundle-Ether** *bundle-id*

**Example:**

```
RP/0/RP0/CPU0:router# show lacp bundle
Bundle-Ether 3
```

(Optional) Shows detailed information about LACP ports and their peers.

## Configuring VLAN Bundles

This section describes how to configure a VLAN bundle. The creation of a VLAN bundle involves three main tasks:

1. Create an Ethernet bundle.
2. Create VLAN subinterfaces and assign them to the Ethernet bundle.
3. Assign Ethernet links to the Ethernet bundle.

These tasks are described in detail in the procedure that follows.



**Note** In order for a VLAN bundle to be active, you must perform the same configuration on both ends of the bundle connection.

**Step 1** **configure**

**Example:**

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

Enters global configuration mode.

**Step 2** **interface Bundle-Ether** *bundle-id*

**Example:**

```
RP/0/RP0/CPU0:router#(config)# interface Bundle-Ether 3
```

Creates and names a new Ethernet link bundle.

This **interface Bundle-Ether** command enters you into the interface configuration submode, where you can enter interface-specific configuration commands. Use the **exit** command to exit from the interface configuration submode back to the normal global configuration mode.

**Step 3**     **ipv4 address** *ipv4-address mask*

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.2.3 255.0.0.0
```

Assigns an IP address and subnet mask to the virtual interface using the **ipv4 address** configuration subcommand.

**Step 4**     **bundle minimum-active links** *links*

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# bundle minimum-active links 2
```

(Optional) Sets the number of active links required before you can bring up a specific bundle.

**Step 5**     **exit**

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# exit
```

Exits the interface configuration submode.

**Step 6**     **interface Bundle-Ether** *bundle-id.vlan-id*

**Example:**

```
RP/0/RP0/CPU0:router#(config)# interface Bundle-Ether 3.1
```

Creates a new VLAN, and assigns the VLAN to the Ethernet bundle you created in Step 2.

Replace the *bundle-id* argument with the *bundle-id* you created in Step 2.

Replace the *vlan-id* with a subinterface identifier. Range is from 1 to 4094 inclusive (0 and 4095 are reserved).

**Note**     When you include the *.vlan-id* argument with the **interface Bundle-Ether** *bundle-id* command, you enter subinterface configuration mode.

**Step 7**     **encapsulation dot1q**

**Example:**

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

Sets the Layer 2 encapsulation of an interface.

**Step 8**     **ipv4 address** *ipv4-address mask*

**Example:**

```
RP/0/RP0/CPU0:router#(config-subif)# ipv4 address 10.1.2.3/24
```

Assigns an IP address and subnet mask to the subinterface.

**Step 9**     **no shutdown**

**Example:**

```
RP/0/RP0/CPU0:router#(config-subif)# no shutdown
```

(Optional) If a link is in the down state, bring it up. The **no shutdown** command returns the link to an up or down state depending on the configuration and state of the link.

**Step 10**    **exit****Example:**

```
RP/0/RP0/CPU0:router(config-subif)# exit
```

Exits subinterface configuration mode for the VLAN subinterface.

**Step 11**    Repeat Step 9 through Step 12 to add more VLANs to the bundle you created in Step 2.

(Optional) Adds more subinterfaces to the bundle.

**Step 12**    **end** or **commit****Example:**

```
RP/0/RP0/CPU0:router(config-subif)# end
```

or

```
RP/0/RP0/CPU0:router(config-subif)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before
exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

**Step 13**    **exit****Example:**

```
RP/0/RP0/CPU0:router(config-subif)# end
```

Exits interface configuration mode.

**Step 14**    **exit****Example:**

```
RP/0/RP0/CPU0:router(config)# exit
```

Exits global configuration mode.

**Step 15**      **configure**

**Example:**

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

Enters global configuration mode.

**Step 16**      **interface {GigabitEthernet | TenGigE} interface-path-id**

**Example:**

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 1/0/0/0
```

Enters interface configuration mode for the Ethernet interface you want to add to the Bundle.

Enter the **GigabitEthernet** or **TenGigE** keyword to specify the interface type. Replace the *interface-path-id* argument with the node-id in the rack/slot/module format.

**Note**          A VLAN bundle is not active until you add an Ethernet interface on both ends of the link bundle.

**Step 17**      **lACP fast-switchover**

**Example:**

```
RP/0/RP0/CPU0:router(config-if)# lACP fast-switchover
```

(Optional) If you enabled 1:1 link protection (you set the value of the **bundle maximum-active links** command to 1) on a bundle with member links running LACP, you can optionally disable the wait-while timer in the LACP state machine. Disabling this timer causes a bundle member link in standby mode to expedite its normal state negotiations, thereby enabling a faster switchover from a failed active link to the standby link.

## VLANs on an Ethernet Link Bundle

You can configure 802.1Q VLAN subinterfaces on 802.3ad Ethernet link bundles. Keep the following information in mind when adding VLANs on an Ethernet link bundle:

- The maximum number of VLANs allowed per bundle is 2048.
- The maximum number of bundled VLANs allowed per router is 2048.



**Note**          The memory requirement for bundle VLANs is slightly higher than standard physical interfaces.

To create a VLAN subinterface on a bundle, include the VLAN subinterface instance with the **interface Bundle-Ether** command, as follows:

```
interface Bundle-Ether interface-bundle-id.subinterface
```

After you create a VLAN on an Ethernet link bundle, the system supports all VLAN subinterface configuration on that link bundle.

VLAN subinterfaces can support Ethernet Flow Points (EFPs) and Layer 3 services.

You can configure Layer 3 VLAN subinterfaces as follows:

```
interface bundle-ether instance.subinterface, encapsulation dot1q xxxxx
```

## Configuration Examples for Link Bundling

This section contains the following examples:

### Example: Configuring an Ethernet Link Bundle

The following example shows how to join two ports to form an EtherChannel bundle that runs LACP:

```
RP/0/RP0/CPU0:Router (config) # config
RP/0/RP0/CPU0:Router (config-if) # interface Bundle-Ether 3
RP/0/RP0/CPU0:Router (config-if) # ipv4 address 1.2.3.4/24
RP/0/RP0/CPU0:Router (config-if) # bundle minimum-active bandwidth 620000
RP/0/RP0/CPU0:Router (config-if) # bundle minimum-active links 1
RP/0/RP0/CPU0:Router (config-if) # exit
RP/0/RP0/CPU0:Router (config-if) # interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:Router (config-if) # bundle id 3 mode active
RP/0/RP0/CPU0:Router (config-if) # no shutdown
RP/0/RP0/CPU0:Router (config) # exit
RP/0/RP0/CPU0:Router (config-if) # interface TenGigE 0/3/0/1
RP/0/RP0/CPU0:Router (config-if) # bundle id 3 mode active
RP/0/RP0/CPU0:Router (config-if) # no shutdown
RP/0/RP0/CPU0:Router (config-if) # exit
```

This example shows the configuration in the case of a mixed speed bundle:

```
RP/0/RP0/CPU0:Router (config) # config
RP/0/RP0/CPU0:Router (config-if) # interface bundle-ether 50
RP/0/RP0/CPU0:Router (config-if) # root
RP/0/RP0/CPU0:Router (config-if) # interface TenGigE 0/0/0/11
RP/0/RP0/CPU0:Router (config-if) # bundle id 50 mode active
RP/0/RP0/CPU0:Router (config-if) # no shutdown
RP/0/RP0/CPU0:Router (config-if) # interface TenGigE 0/0/0/16
RP/0/RP0/CPU0:Router (config-if) # bundle id 50 mode active
RP/0/RP0/CPU0:Router (config-if) # no shutdown
RP/0/RP0/CPU0:Router (config-if) # interface TenGigE 0/0/0/27
RP/0/RP0/CPU0:Router (config-if) # bundleid 50 mode active
RP/0/RP0/CPU0:Router (config-if) # no shutdown
RP/0/RP0/CPU0:Router (config-if) # interface HundredGigE 0/6/0/1
RP/0/RP0/CPU0:Router (config-if) # bundleid 50 mode active
RP/0/RP0/CPU0:Router (config-if) # no shutdown
RP/0/RP0/CPU0:Router (config-if) # root
RP/0/RP0/CPU0:Router (config) # commit
```

```
RP/0/RP0/CPU0:Router(config)# end
```

The following output is shown for the **show bundle bundle-ether** command:

### show bundle bundle-ether50

```
Bundle-Ether50
Status:                               Up
Local links <active/standby/configured>: 4 / 0 / 4
Local bandwidth <effective/available>: 130000000 (130000000) kbps
MAC address (source):                  0011.2233.4458 (Chassis pool)
Inter-chassis link:                    No
Minimum active links / bandwidth:      1 / 1 kbps
Maximum active links:                  64
Wait while timer:                      2000 ms
Load balancing:                        Default
LACP:                                  Operational
  Flap suppression timer:              Off
  Cisco extensions:                    Disabled
mLACP:                                  Not configured
IPv4 BFD:                              Not configured
```

Port	Device	State	Port ID	B/W, kbps
Te0/0/0/11	Local	Active	0x8000, 0x0002	10000000
Link is Active				
Te0/0/0/16	Local	Active	0x8000, 0x0003	10000000
Link is Active				
Te0/0/0/27	Local	Active	0x8000, 0x0004	10000000
Link is Active				
Hu0/6/0/1	Local	Active	0x8000, 0x0001	100000000
Link is Active				

In order to view the weight of a mixed speed bundle, run the **show bundle load-balancing** command. The following is the truncated output of this command.

```
show bundle load-balancing bundle-ether50 location 0/0/cpu0
```

<snip>

```
Bundle-Ether50
Type:           Ether (L3)
Members <current/max>: 4/64
Total Weighting: 13
Load balance:   Default
Locality threshold: 65
Avoid rebalancing? False
Sub-interfaces: 1
```

```
Member Information:
Port:           LON ULID BW
-----
Hu0/6/0/1      0 0 10
Te0/0/0/11     1 1 1
Te0/0/0/16     2 2 1
Te0/0/0/27     3 3 1
```

```
Platform Information:
=====
```

```
* Bundle Summary Information *
-----
```

## Example: Configuring a VLAN Link Bundle

```

Interface      : Bundle-Ether50   Ifhandle      : 0x00000ce0
Lag ID        : 1                Virtual Port   : 255
Number of Members : 4            Local to LC    : Yes
Hash Modulo Index : 13
MGSCP Operational Mode : No

```

## Member Information:

LON	Interface	ifhandle	SFP	port	slot	remote/rack_id
0	Hu0/6/0/1	0x100001c0	648	116	8	0/0
1	Te0/0/0/11	0x04000380	65	9	2	0/0
2	Te0/0/0/16	0x040004c0	67	8	2	0/0
3	Te0/0/0/27	0x04000780	72	4	2	0/0

```
</snip>
```

## Example: Configuring a VLAN Link Bundle

The following example shows how to create and bring up two VLANs on an Ethernet bundle:

```

RP/0/RP0/CPU0:Router(config-subif)# config
RP/0/RP0/CPU0:Router(config-subif)# interface Bundle-Ether 1
RP/0/RP0/CPU0:Router(config-ifsubif)# ipv4 address 1.2.3.4/24
RP/0/RP0/CPU0:Router(config-ifsubif)# bundle minimum-active bandwidth 620000
RP/0/RP0/CPU0:Router(config-if)# bundle minimum-active links
RP/0/RP0/CPU0:Router(config-ifsubif)# exit
RP/0/RP0/CPU0:Router(config-subif)# ip addr 20.2.3.4/24
RP/0/RP0/CPU0:Router(config-subif)# interface Bundle-Ether 1.1
RP/0/RP0/CPU0:Router(config-subif)# encapsulation dot1q 100
RP/0/RP0/CPU0:Router(config-subif) # ip addr 10.2.3.4/24
RP/0/RP0/CPU0:Router(config-subifif)# no shutdown
RP/0/RP0/CPU0:Router(config-subifif)# exit
RP/0/RP0/CPU0:Router(config-if)# interface Bundle-Ether 1.2
RP/0/RP0/CPU0:Router(config-subif)# dot1q vlan 10
RP/0/RP0/CPU0:Router(config-subif)Router # ip addr20.2.3.4/24

RP/0/RP0/CPU0:Router(config-subifif)# no shutdown
RP/0/RP0/CPU0:Router(config-subifif)# exit
RP/0/RP0/CPU0:Router(config)# interface gig 0/1/5/7
RP/0/RP0/CPU0:Router(config-if)# bundle-id 1 mode act
RP/0/RP0/CPU0:Router(config-if)# commit
RP/0/RP0/CPU0:Router(config-if)# exit

```





## CHAPTER 8

# Configuring Traffic Mirroring

This module describes the configuration of the traffic mirroring feature. Traffic mirroring is sometimes called port mirroring, or switched port analyzer (SPAN).

### Feature History for Traffic Mirroring

Release 7.3.1	SPAN to File feature was introduced.
Release 7.2.12	Local SPAN feature was introduced.
Release 7.0.14	Support for the following features was introduced in ERSPAN: <ul style="list-style-type: none"><li>• Configuration of IP DSCP.</li><li>• Tunnel IP.</li><li>• Ability to source ranges of interfaces and SVIs.</li><li>• Sequence bit is set in the GRE header and the value of sequence number is always 0 for ERSPAN packets.</li><li>• ERSPAN and Security ACL should be separate.</li></ul> Support for File Mirroring was introduced.
Release 7.0.11	This feature was introduced.

- [Introduction to Traffic Mirroring, on page 140](#)
- [Restrictions for Traffic Mirroring, on page 149](#)
- [Configuring Traffic Mirroring, on page 150](#)
- [Attaching the Configurable Source Interface, on page 154](#)
- [Introduction to ERSPAN Rate Limit, on page 155](#)
- [Introduction to File Mirroring, on page 157](#)
- [Introduction to Local SPAN, on page 159](#)
- [Traffic Mirroring with DSCP, on page 163](#)
- [Monitor Multiple ERSPAN Sessions with SPAN and Security ACL, on page 168](#)
- [SPAN to File, on page 169](#)
- [Mirroring Forward-Drop Packets, on page 175](#)
- [Traffic Mirroring Configuration Examples, on page 177](#)

- [Troubleshooting Traffic Mirroring, on page 179](#)

## Introduction to Traffic Mirroring

Traffic mirroring, which is sometimes called port mirroring, or Switched Port Analyzer (SPAN) is a Cisco proprietary feature. Traffic mirroring enables you to monitor Layer 3 network traffic passing in, or out of, a set of Ethernet interfaces. You can then pass this traffic to a network analyzer for analysis.

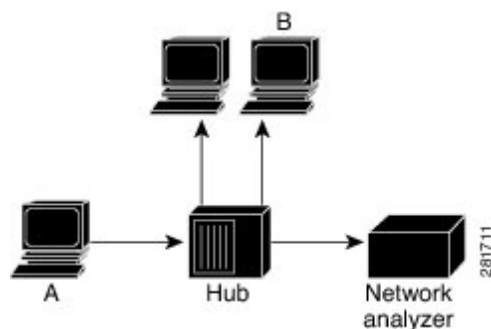
Traffic mirroring copies traffic from one or more Layer 3 interfaces or sub-interfaces. Traffic mirroring then sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device. Traffic mirroring does not affect the switching of traffic on the source interfaces or sub-interfaces. It allows the system to send mirrored traffic to a destination interface or sub-interface.

Traffic mirroring is introduced on switches because of a fundamental difference between switches and hubs. When a hub receives a packet on one port, the hub sends out a copy of that packet from all ports except from the one at which the hub received the packet. In case of switches, after a switch boots, it starts to build up a Layer 2 forwarding table on the basis of the source MAC address of the different packets that the switch receives. After the system builds this forwarding table, the switch forwards traffic that is destined for a MAC address directly to the corresponding port.

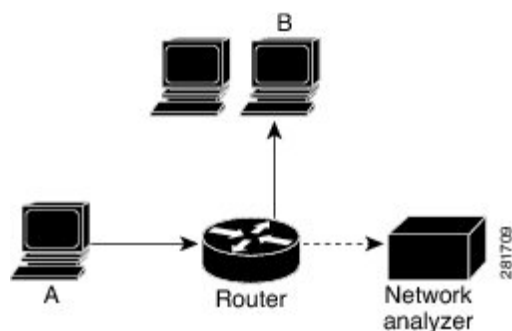
Layer 2 SPAN is not supported on the router.

For example, if you want to capture Ethernet traffic that is sent by host A to host B, and both are connected to a hub, attach a traffic analyzer to this hub. All other ports see the traffic between hosts A and B.

**Figure 8: Traffic Mirroring Operation on a Hub**



On a switch or router, after the system learns host B MAC address, the system forwards the unicast traffic from A to B to the B port. Therefore, the traffic analyzer does not see this traffic.



In this configuration, the traffic analyzer captures only traffic that is flooded to all ports, such as:

- Broadcast traffic
- Multicast traffic with CGMP or Internet Group Management Protocol (IGMP) snooping disabled
- Unknown unicast traffic on a switch

An extra feature is necessary that artificially copies unicast packets that host A sends. This extra feature is traffic mirroring. When traffic mirroring is enabled, the traffic analyzer is attached to a port that is configured to receive a copy of every packet that host A sends. This port is called a traffic mirroring port. The other sections of this document describe how you can fine tune this feature.

## Implementing Traffic Mirroring on the Cisco 8000 Series Routers

### ERSPAN

*Table 19: Feature History Table*

Feature Name	Release Information	Feature Description
Partial Packet Capture Ability for ERSPAN (RX)	Release 7.5.3	With this feature, you can perform partial packet capture in the RX direction.  Earlier, the ability for entire packet capture was available, now you can choose entire or partial packet capture in the RX direction.  Here, partial packet capture is also known as truncation.
ERSPAN over MPLS Traffic	Release 7.5.3	With this release, the router allows you to mirror MPLS traffic and set up the GRE tunnel with the next hop over a labeled path. This feature helps you to remote-monitor the traffic on traffic analyzers.
Higher Payload Analysis with Eight ERSPAN Sessions	Release 7.3.2	With this release, Cisco 8000 Series routers support eight ERSPAN sessions. This functionality helps you analyze higher payloads in real time across Layer 3 domains on your network.
ERSPAN over GRE IPv6	Release 7.3.2	With this release, the router allows you to mirror IPv4 or IPv6 traffic with ERSPAN over GRE IPv6 sessions to monitor traffic on remote traffic analyzers. In earlier releases, ERSPAN traffic monitoring was possible only on IPv4 networks

Encapsulated Remote Switched Port Analyzer (ERSPAN) mirrors traffic on one or more source ports and delivers the mirrored traffic to destination port on another switch or management server. ERSPAN enables network operators to troubleshoot issues in the network in real-time using automated tools that auto-configures ERSPAN parameters on the network devices to send specific flows to management servers for in-depth analysis.

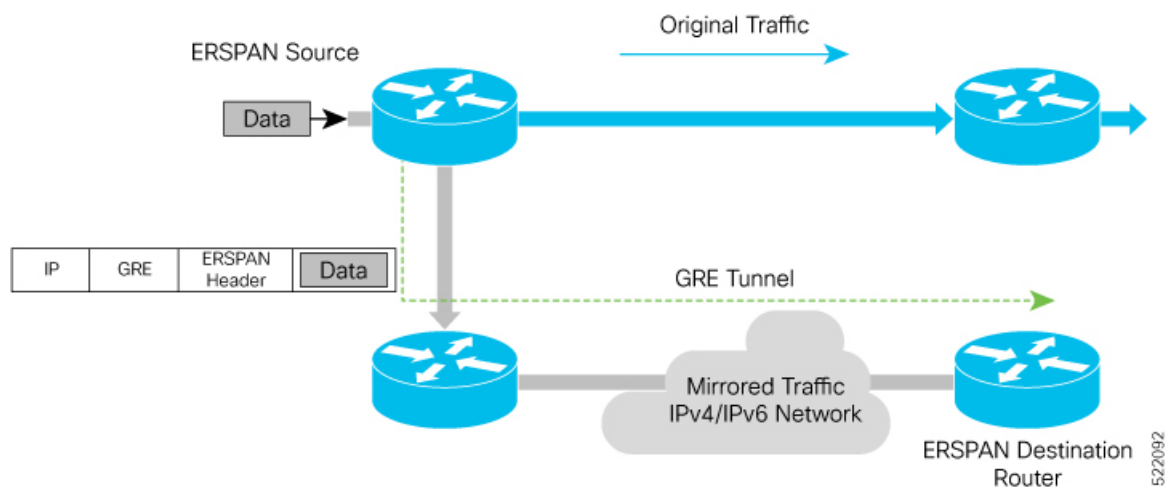
ERSPAN transports mirrored traffic over an IP network. The traffic is encapsulated at the source router and is transferred across the network.

From Cisco IOS XR Software Release 7.5.3 onwards, the packet truncation feature is supported over remote GRE tunnels. You can now get the flexibility to truncate packets and mirror the traffic.

Starting with Cisco IOS XR Software Release 7.0.14, sequence bit is set in the GRE header and the value of sequence number is always 0 for ERSPAN packets.

Starting with Cisco IOS XR Software Release 7.5.3, the sequence number bit will always be set to one and the sequence number field (4 bytes), will always be set to zero.

**Figure 9: ERSPAN over GRE**



### Supported Capabilities

The following capabilities are supported:

- The source interfaces are layer 3 interfaces, such as physical, and bundle interfaces or subinterface.
- The routers mirror IPv4 and IPv6 traffic.
- ERSPAN with GRE IPv4 or IPv6 has tunnel destinations.
- ERSPAN supports only RX direction.
- ERSPAN over GRE IPv4 and IPv6 supports SPAN ACL.
- Supports MPLS traffic mirroring and GRE tunnel configuration with the next hop over a labeled path.
- Each monitor session allows only one destination interface.
- ACL permit or deny entries with capture action are part of mirroring features.
- The next hop interface must be a main interface. It can be a Physical or Bundle interface.

- Supports full packet capture.
- In ERSPAN over GRE IPv6, the **HopLimit** and **TrafficClass** fields in outer IPv6 header are editable under the tunnel configuration.
- The maximum SPAN sessions supported in the Cisco 8000 Router are as follows:.

SPAN Type	7.3.1 and Prior Releases	7.3.2 and Later Releases
ERSPAN (GRE IPv4, GRE IPv6, or GRE IPv4 + GRE IPv6)	4	8
Local SPAN	4	4
SPAN to File	4	4
Combined SPAN (GRE IPv4 + GRE IPv6 + Local SPAN + SPAN to File)	4	8

### Supported Capabilities for ERSPAN Packet Truncation support

The following are the capabilities and requirements:

- Ability to enable the new ERSPAN GREv4 and GREv6 truncation configuration per device.
- Truncation configuration should be on the monitor sessions. Packets received from all sources will only be truncated when you configure the truncation on a monitor session.
- By default, the whole packet will be mirrored without the **mirror first <number>** (truncation size) configuration.
- If the monitor session truncation size is less than the configured-truncation size (343 bytes), then whole packet is mirrored.

If the monitor session truncation size exceeds 343 bytes, the configuration is accepted. However, only 343 bytes truncation size is programmed.

An `ios-msg` is displayed to warn the user.

**Example:** ERSPAN only support 343 bytes truncation size. `monitor-session` with `session_id <id>` will be set to 343 bytes only.

### Restrictions

The following are the ERSPAN and SPAN ACL restrictions:

- The ERSPAN mirror packet is received with a TTL minus 1.  
The mirror packet is not identical to the incoming packet and TTL minus 1 is the expected value in the ERSPAN packet.
- The router mirrors only unicast traffic.  
However, from Cisco IOS XR Software Release 7.5.3 onwards, the router can mirror multicast traffic.
- Remove and re-apply monitor-sessions on all interfaces after modifying the access control list (ACL).

- GRE tunnel is only dedicated to ERSPAN mirrored packets.
- Only ERSPAN TYPE II header is supported. The value of the index field is always 0. The value of the session-ID field is an internal number that is used by the data path to distinguish between sessions.
- Traffic accounting of the ERSPAN mirrored packets is not supported.




---

**Note** You can view the SPAN packet count per session, using the [show monitor-session status internal](#) command.

---

- ERSPAN decapsulation is unsupported.
- In Cisco IOS XR releases 7.5.2 and earlier, ERSPAN over GREv4 and ERSPAN over GREv6 are not supported when MPLS LDP configuration are present on the router.  
However, from Cisco IOS XR Software Release 7.5.3 onwards, the ERSPAN will be functional regardless of any configuration related to MPLS or LDP present on the router.
- MPLS packet mirroring is supported only from Cisco IOS XR Software Release 7.5.3 onwards.
- Due to data path limitation, the source IPv6 addresses of the outer IPv6 header of the ERSPAN packet have only higher 64 bits as valid. The lower 64-bits value is changed to zero. The destination GREv6 IPv6 address should contain all the 128 bits.

#### Restrictions for ERSPAN Packet Truncation support

- From Cisco IOS XR Software Release 7.5.3 onwards, you can truncate the packet size only to a fixed value of 343 bytes.

## Traffic Mirroring Terminology

- Ingress traffic—Traffic that enters the switch.
- Egress traffic—Traffic that leaves the switch.
- Source port—A port that the system monitors with the use of traffic mirroring. It is also called a monitored port.
- Destination port—A port that monitors source ports, usually where a network analyzer is connected. It is also called a monitoring port.
- Monitor session—A designation for a collection of traffic mirroring configurations consisting of a single destination and, potentially, many source interfaces.

## Characteristics of the Source Port

A source port, also called a monitored port, is a switched or routed port that you monitor for network traffic analysis. In a single local or remote traffic mirroring session, you can monitor source port traffic, such as received (Rx) for ingress traffic. Your router can support any number of source ports (up to a maximum number of 800).

A source port has these characteristics:

- It can be any port type, such as Bundle Interface, sub-interface, 100-Gigabit Ethernet, or 400-Gigabit Ethernet.



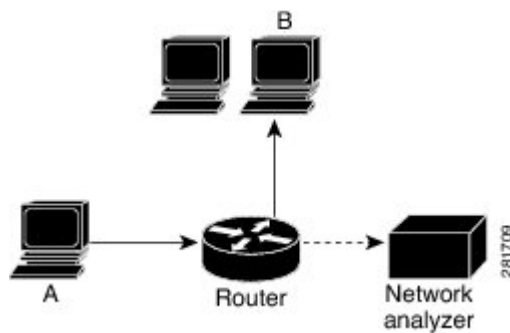

---

**Note** Bridge group virtual interfaces (BVI) are not supported.

---

- Each source port can be monitored in only one traffic mirroring session.
- It cannot be a destination port.
- Each source port can be configured with a direction (ingress) to monitor. For bundles, the monitored direction applies to all physical ports in the group.

**Figure 10: Network Analysis on a Router with Traffic Mirroring**



In the figure above, the network analyzer is attached to a port that is configured to receive a copy of every packet that host A sends. This port is called a traffic mirroring port.

## Characteristics of the Monitor Session

A monitor session is a collection of traffic mirroring configurations consisting of a single destination and, potentially, many source interfaces. For any given monitor session, the traffic from the source interfaces (called *source ports*) is sent to the monitoring port or destination port. If there is more than one source port in a monitoring session, the traffic from the several mirrored traffic streams is combined at the destination port. The result is that the traffic that comes out of the destination port is a combination of the traffic from one or more source ports.

Monitor sessions have these characteristics:

- A single monitor session can have only one destination port.
- A single destination port can belong to only one monitor session.




---

**Note** The destination of ERSPAN monitoring session is a GRE IPv4 or IPv6 tunnel.

---

## Supported Traffic Mirroring Types

The system supports the following traffic mirroring types:

- ACL-based traffic mirroring. The system mirrors traffic that is based on the configuration of the global interface ACL.
- Layer 3 traffic mirroring is supported. The system can mirror Layer 3 source ports.

## ACL-Based Traffic Mirroring

You can mirror traffic that is based on the definition of a global interface access list (ACL). When you are mirroring Layer 3 traffic, the ACL is configured using the **ipv4 access-list** or **ipv6 access-list** command with the **capture** keyword. The **permit** and **deny** commands determine the behavior of regular traffic. The **capture** keyword designates that the packet is to be mirrored to the destination port.

Starting with Cisco IOS XR Software Release 7.0.14, configuration of ERSPAN and security ACL will be separate. Neither of these will have an impact or dependency on the other, but both can be applied simultaneously.

## ERSPAN over GRE IPv6

The ERSPAN over GRE IPv6 feature enables mirroring IPv4 or IPv6 traffic in your network. The router encapsulates the traffic adding an ERSPAN header inside the GRE IPv6 packet. The GRE header of the ERSPAN encapsulated packets have the sequence number set to 0. The router sends the replicated traffic packet to be monitored to the destination through the GRE IPv6 channel to achieve traffic mirroring. The mirrored traffic is sent to remote traffic analyzer for monitoring purposes. For the traffic mirroring to work, the ERSPAN GRE IPv6 tunnel next-hop must have ARP or neighbor resolved. We recommend using the `cef proactive-arp-nd enable` command to configure missing adjacency information for the next hop.

```
Router# configure
Router(config)# cef proactive-arp-nd enable
Router(config)# commit
```

### Configuring ERSPAN over GRE IPv6

#### 1. Enable GRE IPv6 tunnel configuration.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#interface tunnel-ipl
RP/0/RP0/CPU0:router(config-if)#tunnel mode gre ipv6
RP/0/RP0/CPU0:router(config-if)#tunnel source 2001:DB8:1::1
RP/0/RP0/CPU0:router(config-if)#tunnel destination 2001:DB8:2::1
RP/0/RP0/CPU0:router(config-if)#no shut
RP/0/RP0/CPU0:router(config)#commit
```

#### 2. Enable ERSPAN session.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#monitor-session mon1 ethernet
RP/0/RP0/CPU0:router(config-mon)#destination interface tunnel-ipl
RP/0/RP0/CPU0:router(config-mon)#commit
RP/0/RP0/CPU0:router(config-mon)#end
```

#### 3. Configure ERSPAN session under port to be monitored.

```
RP/0/RP0/CPU0:router(config)#interface HundredGigE0/1/0/14
RP/0/RP0/CPU0:router(config-if)#monitor-session mon1 ethernet direction rx-only
RP/0/RP0/CPU0:router(config-if-mon)#exit
RP/0/RP0/CPU0:router(config-if)#exit
RP/0/RP0/CPU0:router(config)#interface Bundle-Ether1
RP/0/RP0/CPU0:router(config-if)#monitor-session mon1 ethernet direction rx-only
RP/0/RP0/CPU0:router(config-if-mon)#exit
RP/0/RP0/CPU0:router(config-if)#exit
```



```
RP/0/RP0/CPU0:router(config)#interface HundredGigE0/1/0/15.100
RP/0/RP0/CPU0:router(config-subif)#monitor-session mon1 ethernet direction rx-only
```

## Verification

Use the `show monitor-session status` command to verify the configuration of the ERSPAN over GRE IPv6 feature.

```
P/0/RP0/CPU0:router#show monitor-session mon1 status
Monitor-session mon1
Destination interface tunnel-ip1
```

```
=====
Source Interface          Dir      Status
-----
Hu0/1/0/14                Rx      Operational
Hu0/1/0/15.100           Rx      Operational
BE1                       Rx      Operational
BE1.1                     Rx      Operational
```

```
RP/0/RP0/CPU0:R1-SF-D#show monitor-session erspan3 status internal
```

```
Thu Jul 15 06:00:14.720 UTC
```

```
Information from SPAN Manager and MA on all nodes:
```

```
Monitor-session erspan3 (ID 0x00000007) (Ethernet)
```

```
SPAN Mgr: Destination interface tunnel-ip372 (0x0f00049c)
```

```
Last error: Success
```

```
Tunnel data:
```

```
Mode: GREoIPv6
```

```
Source IP: 77:3:1::79
```

```
Dest IP: 95::90
```

```
VRF:
```

```
ToS: 100
```

```
TTL: 200
```

```
DFbit: Not set
```

```
0/3/CPU0: Destination interface tunnel-ip372 (0x0f00049c)
```

```
Tunnel data:
```

```
Mode: GREoIPv6
```

```
Source IP: 77:3:1::79
```

```
Dest IP: 95::90
```

```
VRF:
```

```
ToS: 100
```

```
TTL: 200
```

```
DFbit: Not set
```

```
0/RP0/CPU0: Destination interface tunnel-ip372 (0x0f00049c)
```

```
Tunnel data:
```

```
Mode: GREoIPv6
```

```
Source IP: 77:3:1::79
```

```
Dest IP: 95::90
```

```
VRF:
```

```
ToS: 100
```

```
TTL: 200
```

```
DFbit: Not set
```

```
Information from SPAN EA on all nodes:
```

```
Monitor-session 0x00000007 (Ethernet)
```

```
0/3/CPU0: Name 'erspan3', destination interface tunnel-ip372 (0x0f00049c)
```

```
Platform, 0/3/CPU0:
```

```
Monitor Session ID: 7
```

```
Monitor Session Packets: 2427313444
```

```
Monitor Session Bytes: 480591627492
```

## Configuring Partial Packet Capture Ability for ERSPAN (RX)

To configure partial traffic mirroring, use the **mirror first** command in monitor session configuration mode.

`Mirror first <number>`: Configures the size of truncation packets for an ERSPAN session

Use the following command to create a ERSPAN monitor session for mirroring the packets:

```
monitor-session <name> [ethernet]
destination interface tunnel-ip <number>
mirror first <number>
    traffic-class <traffic-class>
```

### Configuration Example

Use the following command to create a ERSPAN monitor session for mirroring packets to Tunnel-IP 30 with truncation enabled:

```
monitor-session mon1 ethernet
    destination interface tunnel-ip 30
    mirror first 343
!
```

Attach the session to the interfaces using the following configuration:

```
interface <>
    monitor-session session-name ethernet direction rx-only|tx-only|both | acl [acl_name]
```

### Running Configuration

```
interface tunnel-ip30
    tunnel mode gre ipv4
    tunnel source 2.2.2.2
    tunnel destination 200.0.0.2
!

interface HundredGigE0/0/0/12
    ipv4 address 12.0.0.2 255.255.255.0
    monitor-session mon1 ethernet direction rx-only
!
```

### Verification

The **show monitor-session status internal** displays the size of the programmed truncation.

Example:

```
Router#show monitor-session mon1 status internal
Fri Apr 12 18:50:45.006 UTC
Information from SPAN Manager and MA on all nodes:
Packet truncation size: 343B
Monitor-session mon1 (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface Tunnel-IP 20 (0x0f000250)
        Last error: Success

Information from SPAN EA on all nodes:
Monitor-session 0x00000001 (Ethernet)
0/RP0/CPU0: Name 'mon1', destination interface Tunnel-IP 20 (0x0f000250)
Platform, 0/RP0/CPU0:

    Monitor Session Packets: 142462

    Monitor Session Bytes: 7653237
```

## ERSPAN Traffic to a Destination in a Non-Default VRF

Table 20: Feature History Table

Feature Name	Release Information	Description
ERSPAN Traffic to a Destination in a Non-Default VRF	Release 7.5.2	Encapsulated Remote Switched Port Analyzer (ERSPAN) now transports mirrored traffic through GRE tunnels with multiple VRFs, helping you design your network with multiple Layer 3 partitions.  In earlier releases, ERSPAN transported mirrored traffic through GRE tunnels that belonged to only default VRF.

## Restrictions for Traffic Mirroring

The system supports the following forms of traffic mirroring:

- Mirroring traffic to a GRE IPv4 or IPv6 tunnel (also known as Encapsulated Remote Switched Port Analyzer [ER-SPAN] in Cisco IOS Software). The system allows 8 monitor sessions for ERSPAN, 4 monitor sessions for Local SPAN, and 4 monitor sessions for SPAN to File. The total number of monitor sessions for all SPAN features is 8.
- The system does not support traffic mirroring counters per interface.
- The system does not support bundle member interfaces as sources for mirroring sessions.
- ERSPAN tunnel statistics is not supported.

The following general restrictions apply to traffic mirroring using ACLs:

- Configure ACLs on the source interface to avoid default mirroring of traffic. If a Bundle interface is a source interface, configure the ACLs on the bundle interface (not bundle members).

The following restrictions apply to ERSPAN ACL:

- ERSPAN next-hop must have ARP resolved.
  - Any other traffic or protocol triggers ARP.
- ERSPAN decapsulation is not supported.
- ERSPAN does not work if the GRE next hop is reachable over subinterface. For ERSPAN to work, the next hop must be reachable over the main interface.
- When you use the same ACEs defined in both the IPv4 and IPv6 ACLs, the router doesn't perform ERSPAN mirroring for the ACLs with the lowest priority set as 2 ms.
- However, from Cisco IOS XR Software Release 7.5.3 onwards, GRE next hop can be resolved over subinterface or the main interface.

### Modifying ERSPAN monitor-session configuration

When you modify the ERSPAN monitor-session configuration, the **show configuration** and **show configuration commit changes** command outputs differ. Specifically, the **show configuration commit changes** command output displays some extraneous ACL commands deleted and added back. This modified output doesn't impact your configuration or affect performance. This issue is fixed in Cisco IOS XR Release 7.5.1.

The following example highlights the extraneous ACL commands under the **show configuration commit changes** command output.

```
Router(config)#interface HundredGigE0/1/0/0
Router(config-if)#no monitor-session ERSPANtun2005
Router(config-if)#monitor-session ERSPANtun2 ethernet direction rx-only port-level
Router(config-if-mon)#acl
Router(config-if-mon)#acl ipv4 erspan-filter
Router(config-if-mon)#acl ipv6 erspan-filter-ipv6
Router(config-if-mon)#
Router(config-if-mon)#show configuration
Building configuration...
!! interface HundredGigE0/1/0/0
   monitor-session ERSPANtun2 ethernet direction rx-only port-level
   acl
   acl ipv4 erspan-filter
   acl ipv6 erspan-filter-ipv6
   !
   !
end

Router(config-if-mon)#commit
Router(config-if-mon)#end
Router#sh configuration commit changes las 1
Building configuration...
!!
interface HundredGigE0/1/0/0
  no monitor-session ERSPANtun2005 ethernet direction rx-only port-level
  monitor-session ERSPANtun2 ethernet direction rx-only port-level
  no acl
  acl
  no acl ipv4 erspan-filter
  acl ipv4 erspan-filter
  no acl ipv6 erspan-filter-ipv6
  acl ipv6 erspan-filter-ipv6
  !
  !
end
```

## Configuring Traffic Mirroring

These tasks describe how to configure traffic mirroring:

### Configuring ACLs for Traffic Mirroring

This section describes the configuration for creating ACLs for traffic mirroring. You must configure the global interface ACLs by using one of the following commands with the **capture** keyword:

- **ipv4 access-list**

- **ipv6 access-list**



**Note** Starting with Cisco IOS XR Software Release 7.0.14, ACL feature will provide a support of separate ACL configuration for SPAN.

### Configuration

- **Security ACL**

Use the following configuration to configure ACLs for traffic mirroring.

```
/* Create an IPv4 ACL (TM-ACL) for traffic mirroring */
Router(config)# ipv4 access-list TM-ACL
Router(config-ipv4-acl)# 10 permit udp 10.10.10.0 0.0.0.255 eq 10 any capture
Router(config-ipv4-acl)# 20 permit udp 10.10.10.0 0.0.0.255 eq 20 any
Router(config-ipv4-acl)# exit
Router(config)# commit

/* Apply the traffic monitoring to SPAN source interface */
Router(config)# interface HundredGigE0/0/0/12
Router(config-if)# monitor-session mon1 ethernet direction rx-only port-level acl
Router(config-if)# ipv4 access-group TM-ACL ingress
!
```

Use the following configuration as an example to deny data forwarding for an ACE entry, but still mirror the traffic:

```
ipv4 access-list acl1
10 deny ipv4 any 2.1.0.0/16 capture
20 permit ipv4 any any
!
```

If `acl1` is attached to the interface as shown below:

```
RP/0/RP0/CPU0(config-if)# ipv4 access-group acl1 ingress
```

Data Traffic to 2.1.0.0/16 is dropped. Mirroring happens only if `icmp-off` keyword is added to the ACE as shown below. If this keyword is not added, mirroring does not take place. Furthermore, the `icmp-off` workaround is applicable only to security ACL.

```
ipv4 access-list acl1
10 deny ipv4 any 2.1.0.0/16 capture icmp-off
20 permit ipv4 any any
!
```

- **SPAN ACL**

- SPAN ACL does not support User Defined Fields (UDF).
- Deny action in SPAN ACL is ignored, and no packet drops from SPAN ACL. Deny ACEs will be internally converted to permit ACEs. Packets will also be mirrored.
- There is no implicit deny-all entry in SPAN ACL.
- IPV6 ACL is required for mirroring IPV6 packet, if IPV4 ACL is configured, and vice versa. This follows the same structure as Security ACL with IPv4 and IPv6 mirror options.

The maximum scale for SPAN ACL ID for fixed and centralized chassis is 3/slice pair and 9/NP. For distributed chassis, the maximum scale for SPAN ACL ID is 6/NP.

Use the following configuration to enable traffic mirroring with ACLs.

```
/* Create a SPAN IPv4 ACL (v4-monitor-acl) for traffic mirroring */
Router(config)# ipv4 access-list v4-monitor-acl
Router(config-ipv4-acl)# 10 permit udp 20.1.1.0 0.0.0.255 eq 10 any
Router(config-ipv4-acl)# 20 permit udp 30.1.1.0 0.0.0.255 eq 20 any
Router(config-ipv4-acl)# exit
Router(config)# commit

/*Create a SPAN IPv6 ACL (v6-monitor-acl) for traffic mirroring */
Router(config)# ipv6 access-list v6-monitor-acl
Router(config-ipv6-acl)# 10 permit ipv6 host 120:1:1::1 host 130:1:1::1
Router(config-ipv6-acl)# exit

/* Apply the traffic monitoring to SPAN source interface */
Router(config)# interface HundredGigE0/0/0/12
Router(config-if)# monitor-session mon1 ethernet direction rx-only
Router(config-if)# acl ipv4 v4-monitor-acl
Router(config-if)# acl ipv6 v6-monitor-acl!
```




---

**Note** The `capture` keyword which is required for Security ACL for SPAN to work, is optional for SPAN ACL.

---

Use the `show access-lists [ipv4 | ipv6] acl-name hardware ingress span [detail | interface | location | sequence | verify] location x command` to display ACL information:

```
Router# show access-lists ipv4 v4span1 hardware ingress span interface bundle-Ether 100
location 0/3/cpu0
ipv4 access-list v4span1
10 permit ipv4 host 51.0.0.0 host 101.0.0.0
20 permit ipv4 host 51.0.0.1 host 101.0.0.1
30 permit ipv4 host 51.0.0.2 any
40 permit ipv4 any host 101.0.0.3
50 permit ipv4 51.0.1.0 0.0.0.255 101.0.1.0 0.0.0.255
60 permit ipv4 51.0.2.0 0.0.0.255 101.0.2.0 0.0.0.255 precedence critical
```

## Troubleshooting ACL-Based Traffic Mirroring

Take note of these configuration issues:

- Even when the system configures the `acl` command on the source mirroring port, if the ACL configuration command does not use the `capture` keyword, the system does not mirror traffic.
- If the ACL configuration uses the `capture` keyword, but you have not configured the `acl` command on the source port, the system mirrors the traffic, but does not apply access list configuration.

This example shows both the `capture` keyword in the ACL definition and the `acl` command that is configured on the interface:

```
/* Create an IPv4 ACL (TM-ACL) for traffic mirroring */
Router(config)# ipv4 access-list TM-ACL
Router(config-ipv4-acl)# 10 permit udp 10.1.1.0 0.0.0.255 eq 10 any capture
Router(config-ipv4-acl)# 20 permit udp 10.1.1.0 0.0.0.255 eq 20 any
```

Apply the traffic monitoring to interface

```
Router(config)#interface HundredGigE0/0/0/12
Router(config-if)# monitor-session mon1 ethernet direction rx-only port-only acl
Router(config-if)# ipv4 access-group TM-ACL ingress
```

## Flexible CLI for ERSPAN

Starting with Cisco IOS XR Software Release 7.0.14, ERSPAN can be configured using flexible CLI. This CLI is a single configuration object containing all the properties of an ERSPAN session, tunnel properties, and the list of source interfaces, which can be easily removed and re-added. Flexible CLI minimises risk of user error and promotes operational simplicity.

Configure a flexible CLI group in ERSPAN containing:

- Global ERSPAN session configuration
- Tunnel interface configuration
- ERSPAN source attachment configuration, applied to a regexp of interface names



**Note** The flexible CLI group contains only the session and interface properties. The session and interface objects themselves must be created in the configuration as usual.

The following example shows a global flexible CLI configuration:

```
group erspan-group-foo
  monitor-session 'foo' ethernet /* Global configuration */
    destination interface tunnel-ip0
  !
  interface 'tunnel-ip0' /* Tunnel interface configuration */
    tunnel tos 10
    tunnel mode gre ipv4
    tunnel source 10.10.10.1
    tunnel destination 20.20.20.2
  !
  interface 'GigabitEthernet0/0/0/[0-3]' /* Interface configuration */
    monitor-session foo ethernet
  !
end-group
```

To enable all ERSPAN configurations, execute `apply-group erspan-group-foo` command. To disable ERSPAN configuration, delete this command.



**Note** The following three keywords are regular expressions and must be quoted:

- Definition of session name (example: `foo`)
- Definition of tunnel name (example: `tunnel-ip0`)
- Set of source interface names (example: `GigabitEthernet0/0/0/[0-3]`)

Use the `show running-config inheritance` command to view the final configuration after the group is expanded, and the `show monitor-session status` to check the operational state of ERSPAN session.

# Attaching the Configurable Source Interface

## Step 1 **configure**

### Example:

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

Enters global configuration mode.

## Step 2 **interface type number**

### Example:

```
RP/0/RP0/CPU0(config)# interface HundredGigE 0/1/0/10/0/1/0
```

Enters interface configuration mode for the specified source interface. The interface number is entered in *rack/slot/module/port* notation. For more information about the syntax for the router, use the question mark (?) online help function.

## Step 3 **ipv4 access-group acl-name {ingress | egress}**

### Example:

```
RP/0/RP0/CPU0(config-if)# ipv4 access-group acl1 ingress
```

Controls access to an interface.

## Step 4 **monitor-session session-name ethernet direction rx-only port-level**

### Example:

```
RP/0/RP0/CPU0(config-if)# monitor-session mon1 ethernet direction rx-only port-level acl  
RP/0/RP0/CPU0(config-if-mon)#
```

Attaches a monitor session to the source interface and enters monitor session configuration mode.

**Note** **rx-only** specifies that only ingress traffic is replicated.

## Step 5 **acl**

### Example:

```
RP/0/RP0/CPU0(config-if-mon)# acl
```

Specifies that the traffic mirrored is according to the defined ACL.

**Note** If an ACL is configured by name then this overrides any ACL that may be configured on the interface.

## Step 6 **exit**

### Example:

```
RP/0/RP0/CPU0(config-if-mon)# exit  
RP/0/RP0/CPU0(config-if)#
```



Exits monitor session configuration mode and returns to interface configuration mode.

**Step 7** **end** or **commit****Example:**

```
RP/0/RP0/CPU0(config-if)# end
```

or

```
RP/0/RP0/CPU0(config-if)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting (yes/no/cancel)?  
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

**Step 8** **show monitor-session [session-name] status [detail] [error]****Example:**

```
RP/0/RP0/CPU0# show monitor-session status
```

Displays information about the monitor session.

## Introduction to ERSPAN Rate Limit

With ERSPAN rate limit feature, you can monitor traffic flow through any IP network. This includes third-party switches and routers.

ERSPAN operates in the following modes:

- ERSPAN Source Session – box where the traffic originates (is SPANned).
- ERSPAN Termination Session or Destination Session – box where the traffic is analyzed.

This feature provides rate limiting of the mirroring traffic. With rate limiting, you can limit the amount of traffic to a specific rate, which prevents the network and remote ERSPAN destination traffic overloading. Be informed, if the rate-limit exceeds then the system may cap or drop the monitored traffic.

You can configure the QoS parameters on the traffic monitor session.

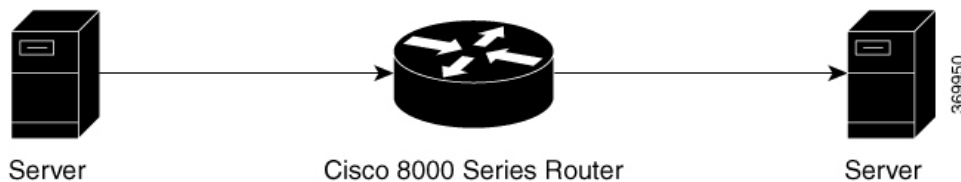
- Traffic Class (0 through 7)
  - Traffic class 0 has the lowest priority and 7 the highest.
  - The default traffic class is the same as that of the original traffic class.

### Benefits

With ERSPAN rate limit feature, you can limit the mirrored traffic and use the mirrored traffic for data analysis.

## Topology

Figure 11: Topology for ERSPAN Rate Limit



The encapsulated packet for ERSPAN is in ARPA/IP format with GRE encapsulation. The system sends the GRE tunneled packet to the destination box identified by an IP address. At the destination box, SPAN-ASIC decodes this packet and sends out the packets through a port. ERSPAN rate limit feature is applied on the router interface to rate limit the monitored traffic.

The intermediate switches carrying ERSPAN traffic from source session to termination session can belong to any L3 network.

## Configure ERSPAN Rate Limit

Use the following steps to configure ERSPAN rate limit:

```

monitor-session ERSPAN ethernet
destination interface tunnel-ipl
!

RP/0/RP0/CPU0:pyke-008#sh run int tunnel-ip 1

interface tunnel-ipl
ipv4 address 4.4.4.1 255.255.255.0
tunnel mode gre ipv4
tunnel source 20.1.1.1
tunnel destination 20.1.1.2
!

RP/0/RP0/CPU0:pyke-008#sh run int hundredGigE 0/0/0/16

interface HundredGigE0/0/0/16
ipv4 address 215.1.1.1 255.255.255.0
ipv6 address 3001::2/64
monitor-session ERSPAN ethernet direction rx-only port-level
  acl
!
ipv4 access-group ACL6 ingress
  
```

## Running Configuration

```
!!A traffic class needs to be configured under the monitor session.
monitor-session mon2 ethernet
destination interface tunnel-ip30
traffic class 5
```

A shaper needs to be configured for this traffic class:

```
policy-map m8
class TC1
  bandwidth percent 11
  !
class TC2
  bandwidth percent 12
  !
class TC3
  bandwidth percent 13
  !
class TC4
  bandwidth percent 14
  !
class TC5
  shape average percent 15
  !
class TC6
  bandwidth percent 16
  !
class TC7
  bandwidth percent 17
```

This policy-map has to be installed on the interface over which the mirrored traffic is sent in the egress direction:

```
interface TenGigE0/6/0/9/0
service-policy output m8
```

## Verification

```
RP/0/RP0/CPU0:ios#show monitor-session FOO status detail
Wed May 2 15:14:05.762 UTC
Monitor-session FOO
Destination interface tunnel-ip100
Source Interfaces
-----
TenGigE0/6/0/4/0
Direction: Both
Port level: True
ACL match: Disabled
```

# Introduction to File Mirroring

Prior to Cisco IOS XR Software Release 7.2.1 7.0.14, the router did not support file mirroring from active RP to standby RP. Administrators had to manually perform the task or use EEM scripts to sync files across active RP and standby RP. Starting with Cisco IOS XR Software Release 7.2.1 7.0.14, file mirroring feature enables the router to copy files or directories automatically from `/harddisk:/mirror` location in active RP to `/harddisk:/mirror` location in standby RP or RSP without user intervention or EEM scripts.

Two new CLIs have been introduced for the file mirroring feature:

- `mirror enable`

The `/harddisk:/mirror` directory is created by default, but file mirroring functionality is only enabled by executing the `mirror enable` command from configuration terminal. Status of the mirrored files can be viewed with `show mirror status` command.

- **mirror enable checksum**

The `mirror enable checksum` command enables MD5 checksum across active to standby RP to check integrity of the files. This command is optional.

## Limitations

The following limitations apply to file mirroring:

- Supported only on Dual RP systems.
- Supports syncing only from active to standby RP. If files are copied into standby `/harddisk:/mirror` location, it won't be synced to active RP.
- A slight delay is observed in `show mirror` command output when mirror checksum configuration is enabled.
- Not supported on multichassis systems.

## Configure File Mirroring

File mirroring has to be enabled explicitly on the router. It is not enabled by default.

```
RP/0/RSP0/CPU0:router#show run mirror
```

```
Thu Jun 25 10:12:17.303 UTC
mirror enable
mirror checksum
```

Following is an example of copying running configuration to `harddisk:/mirror` location:

```
RP/0/RSP0/CPU0:router#copy running-config harddisk:/mirror/run_config
Wed Jul 8 10:25:51.064 PDT
Destination file name (control-c to abort): [/mirror/run_config]?
Building configuration..
32691 lines built in 2 seconds (16345)lines/sec
[OK]
```

### Verification

To verify the syncing of file copied to mirror directory, use the `show mirror` command.

```
RP/0/RSP0/CPU0:router#show mirror
Wed Jul 8 10:31:21.644 PDT
% Mirror rsync is using checksum, this show command may take several minutes if you have
many files. Use Ctrl+C to abort
MIRROR DIR: /harddisk:/mirror/
% Last sync of this dir ended at Wed Jul 8 10:31:11 2020
Location      |Mirrored |MD5 Checksum                |Modification Time
-----
run_config |yes      |76fc1b906bec4fe08ecda0c93f6c7815 |Wed Jul 8 10:25:56 2020
```

If checksum is disabled, `show mirror` command displays the following output:

```
RP/0/RSP0/CPU0:router#show mirror
Wed Jul 8 10:39:09.646 PDT
```

```

MIRROR DIR: /harddisk:/mirror/
% Last sync of this dir ended at Wed Jul  8 10:31:11 2020
Location   |Mirrored |Modification Time
-----|-----|-----
run_config |yes      |Wed Jul  8 10:25:56 2020

```

If there is a mismatch during the syncing process, use `show mirror mismatch` command to verify.

```

RP/0/RP0/CPU0:router# show mirror mismatch
Wed Jul  8 10:31:21.644 PDT
MIRROR DIR: /harddisk:/mirror/
% Last sync of this dir ended at Wed Jul  8 10:31:11 2020
Location |Mismatch Reason |Action Needed
-----|-----|-----
test.txt |newly created item. |send to standby

```

# Introduction to Local SPAN

## Local SPAN Overview

Local SPAN is the most basic form of traffic mirroring. In Local SPAN, both mirror source and mirror destination interfaces are present on the same router.

## Local SPAN Supported Capabilities

The following capabilities are supported for Local SPAN:

- Only ingress traffic.
- The destination interface can only be an L2 or L3 physical main interface.
- The following interfaces are configured as sources for a Local SPAN session:
  - L3 physical main and sub-interface and bundle main and sub-interface.
  - L2 ethernet interfaces: Ethernet Flow Point (EFP) and trunk
  - BVI interface
- The following types of traffic are mirrored Local SPAN:
  - IPv4, IPv6, and MPLS
  - IP-in-IP
- Extended ACL to reduce mirrored traffic throughput
- Traffic shaping on the destination interface
- Session statistics. There's one counter for all types of traffic, that is, IPv4, IPv6, and MPLS.
- Up to four Local SPAN sessions. This session number is shared between ERSPAN, Local SPAN, and SPAN to File features.
- Up to 1000 source interfaces

## Local SPAN Restrictions

The following are the restrictions for Local SPAN:

- Egress mirroring isn't supported
- The physical interface used as destination can't be a bundle member link
- GRE tunnel isn't supported as source interface and destination interface
- Port-level monitoring isn't supported
- Per-source interface mirroring statistics isn't supported. However, SPAN session statistics are supported. The session statistics would contain total number of packets mirrored by the session.
- A destination interface can't be a mirrored source interface and vice versa.
- ACL for Local SPAN is only applied in ingress direction.
- If ACL keyword is present in monitor-session configuration for an interface but no ACL is applied to that interface, traffic packets won't be mirrored
- No ACL support for MPLS traffic
- No support for NetFlow or sFlow configuration on the same interface which has Local SPAN session already configured.

## Configuring Local SPAN

Configuring Local SPAN consists of 2 parts:

### 1. Creating a local SPAN session

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#monitor-session mon1 ethernet
RP/0/RP0/CPU0:router(config-mon)#destination interface HundredGigE0/1/0/0
RP/0/RP0/CPU0:router(config-mon)#commit
RP/0/RP0/CPU0:router(config-mon)#end
RP/0/RP0/CPU0:router#
```

### 2. Attaching the SPAN session to an interface

```
RP/0/RP0/CPU0:router(config-mon)#interface HundredGigE0/1/0/2
RP/0/RP0/CPU0:router(config-if)# monitor-session mon1 ethernet direction rx-only
RP/0/RP0/CPU0:router(config-if-mon)# no shut
RP/0/RP0/CPU0:router(config-if)#!
RP/0/RP0/CPU0:router(config-if)#
RP/0/RP0/CPU0:router(config-if)#interface Bundle-Ether1
RP/0/RP0/CPU0:router(config-if)# monitor-session mon1 ethernet direction rx-only
RP/0/RP0/CPU0:router(config-if-mon)# no shutdown
RP/0/RP0/CPU0:router(config-if)#!
RP/0/RP0/CPU0:router(config-if)#

RP/0/RP0/CPU0:monitor(config-if)#
RP/0/RP0/CPU0:monitor(config-if)#interface HundredGigE0/1/0/14.100
RP/0/RP0/CPU0:monitor(config-subif)# monitor-session mon1 ethernet direction rx-only
RP/0/RP0/CPU0:monitor(config-if-mon)# no shut
RP/0/RP0/CPU0:monitor(config-subif)#!
RP/0/RP0/CPU0:monitor(config-subif)#
RP/0/RP0/CPU0:monitor(config-subif)#interface Bundle-Ether1.1
RP/0/RP0/CPU0:monitor(config-subif)# monitor-session mon1 ethernet direction rx-only
```

```
RP/0/RP0/CPU0:monitor(config-if-mon)# no shut
RP/0/RP0/CPU0:monitor(config-subif)#!
RP/0/RP0/CPU0:monitor(config-subif)#commit
```

### Verification

```
RP/0/RP0/CPU0:router#show monitor-session status
Monitor-session mon1
Destination interface HundredGigE0/1/0/0
=====
Source Interface      Dir      Status
-----
Hu0/1/0/2            Rx      Operational
Hu0/1/0/14.100       Rx      Operational
BE1                  Rx      Operational
BE1.1                Rx      Operational
```

Execute the `show monitor-session status internal` command for session statistics:

```
RP/0/RP0/CPU0:router#show monitor-session status internal
Thu Aug 13 20:05:23.478 UTC
Information from SPAN Manager and MA on all nodes:
Monitor-session mon1 (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface HundredGigE0/1/0/0 (0x00800190)
          Last error: Success
0/1/CPU0: Destination interface HundredGigE0/1/0/0 (0x00800190)
0/RP0/CPU0: Destination interface HundredGigE0/1/0/0 (0x00800190)
Information from SPAN EA on all nodes:
Monitor-session 0x00000001 (Ethernet)
0/1/CPU0: Name 'mon1', destination interface HundredGigE0/1/0/0 (0x00800190)
Platform, 0/1/CPU0:

Monitor Session ID: 1
Monitor Session Packets: 32
Monitor Session Bytes: 4024

0/2/CPU0: Name 'mon1', destination interface HundredGigE0/1/0/0 (0x00800190)
Platform, 0/2/CPU0:

Monitor Session ID: 1
Monitor Session Packets: 0
Monitor Session Bytes: 0
```

## Local SPAN with ACL

Local SPAN with ACL is used to filter and mirror ingress traffic. Only Access Control Entries (ACEs) with `capture` keyword are considered for mirroring. Both permit and deny packets are captured if the ACE contains `capture` keyword. Per interface, only one IPv4 ingress ACL and one IPv6 ingress ACL is allowed.

### Configuring Local SPAN with ACL

Use the following configuration to enable local SPAN with IPv4 ACLs:

1. Configure ACLs for traffic mirroring.

```
Router(config)# ipv4 access-list acl1
Router(config-ipv4-acl)# 10 permit ipv4 25.0.0.0 0.0.0.255 any capture
Router(config-ipv4-acl)# 20 permit ipv4 20.0.0.0 0.0.0.255 any
Router(config-ipv4-acl)# 30 permit ipv4 131.1.1.0 0.0.0.255 any capture
Router(config-ipv4-acl)# 40 permit ipv4 191.1.1.0 0.0.0.255 any capture
```

2. Apply the traffic monitoring to an interface.

```

Router(config)# interface HundredGigE0/1/0/2
Router(config-if)# ipv4 address 131.1.1.2 255.255.255.0
Router(config-if)# monitor-session mon1 ethernet direction rx-only port-level
Router(config-if-mon)# acl
Router(config-if-mon)# ipv4 access-group acl1 ingress

```

### Verification

```

RP/0/RP0/CPU0:ios#show running-config ipv4 access-list acl1
Thu Aug 13 20:22:54.388 UTC
ipv4 access-list acl1
 10 permit ipv4 22.0.0.0 0.0.0.255 any capture
 20 permit ipv4 20.0.0.0 0.0.0.255 any
 30 permit ipv4 131.1.1.0 0.0.0.255 any capture
 40 deny ipv4 181.1.1.0 0.0.0.255 any capture
!
```

Use the following configuration to enable local SPAN with IPv6 ACLs:

#### 1. Configure ACLs for traffic mirroring.

```

Router(config)# ipv6 access-list acl2
Router(config-ipv6-acl)# 10 permit ipv6 10:1:1::2/64 any capture
Router(config-ipv6-acl)# 20 permit ipv6 10:1:1::3/64 any
Router(config-ipv6-acl)# 30 permit ipv6 10:1:1::4/64 any capture

```

#### 2. Apply the traffic monitoring to an interface.

```

Router(config)# interface HundredGigE0/1/0/3
Router(config-if)# ipv6 address 10:1:1::5/64
Router(config-if)# monitor-session mon2 ethernet direction rx-only port-level
Router(config-if-mon)# acl
Router(config-if-mon)# ipv6 access-group acl2 ingress

```

### Verification

```

RP/0/RP0/CPU0:ios#show running-config ipv6 access-list acl2
Thu Aug 14 20:22:54.388 UTC
ipv6 access-list acl2
 10 permit ipv6 10:1:1::2/64 any capture
 20 permit ipv6 10:1:1::3/64 any
 30 permit ipv6 10:1:1::4/64 any capture
!
```

## Local SPAN Rate Limit

Local SPAN rate limiting takes place at the session level and not at source interface level. For rate limiting, local SPAN session should configure a traffic class. This traffic class is used to shape traffic on an egress interface. A QoS policy is applied to the egress interface over which mirrored traffic is sent.

### Example for Local SPAN Rate Limit Configuration

```

Router# monitor-session mon2 ethernet
destination interface HundredGigE0/1/0/19
traffic-class 5

class-map match-any TC5
match traffic-class 5
end-class-map

policy-map shape-foo
class TC5 /* This has to match the class that was configured on monitor session */
shape average percent 15

```



```

class class-default

interface HundredGigE0/1/0/19    /* This is the egress interface over which mirrored packets
are sent */
service-policy output shape-foo

```

## Traffic Mirroring with DSCP

Differentiated Service Code Point (DSCP) value of Differentiated Services (DS) field in IP packet is used to classify the traffic in the network. DS field formerly known as Type of Service (ToS). You can set the DSCP value in the six most significant bits of the differentiated services (DS) field of the IP header, thereby giving  $2^6 = 64$  different values (0 to 63). These six bits affect the Per Hop Behavior (PHB) and hence affects how a packet is moved forward. The default value of DSCP is zero (0). DSCP was defined under RFC 2474.

Following the principle of traffic classification, DSCP places a particular packet into a limited number of traffic classes. Similarly, the router is also informed about the DSCP values and the router can prioritize the packet in traffic flow.

Refer the table to know more about the service class names defined in [RFC 2474](#).

**Table 21: DSCP, DS, and ToS values**

DSCP Value in Decimal	DS Binary	DS Hex	DSCP Name	DS/ToS Value	Service Class
0	000000	0x00	DF/CS0	0	Standard
-	-	-	none	2	
1	000001	0x01	None	4	
1	000001	0x01	LE	4	Lower-effort
2	000010	0x02	None	8	
4	000100	0x04	None	16	
8	001 000	0x08	CS1	32	Low-priority data
10	001 010	0x0a	AF11	40	High-throughput data
12	001 100	0x0c	AF12	48	High-throughput data
14	001 110	0x0e	AF13	56	High-throughput data
16	010 000	0x10	CS2	64	OAM
18	010 010	0x12	AF21	72	Low-latency data
20	010 100	0x14	AF22	80	Low-latency data
22	010 010	0x16	AF23	88	Low-latency data
24	011 000	0x18	CS3	96	Broadcast video
26	011 000	0x1a	AF31	104	Multimedia streaming
28	011 100	0x1c	AF32	112	Multimedia streaming
30	011 110	0x1e	AF33	120	Multimedia streaming

32	100 000	0x20	CS4	128	Real-timeinteractive
34	100 010	0x22	AF41	136	Multimedia conferencing
36	100 100	0x24	AF42	144	Multimedia conferencing
38	100 110	0x26	AF43	152	Multimedia conferencing
40	101 000	0x28	CS5	160	Signaling(IP telephony, etc)
44	101 100	0x2c	Voice-admit	176	
46	101 110	0x2e	EF	184	Telephony
48	110 000	0x30	CS6	192	Networkrouting control
56	111 000	0x38	CS7	224	“reserved”

## DSCP Marking on Egress GRE Tunnel in ERSPAN

Table 22: Feature History Table

Feature Name	Release Information	Feature Description
DSCP Marking on Egress GRE Tunnel in ERSPAN	Release 7.5.4	You can now set or modify Differentiated Service Code Point (DSCP) value on the ERSPAN GRE tunnel header. This feature allows you to control the QoS for your network's ERSPAN GRE tunnel traffic and eases the effort to control your customers' bandwidth across next-hop routers.

Starting Cisco IOS XR Software Release 7.5.4, you can set or modify the DSCP marking on the ERSPAN GRE tunnels. ERSPAN uses GRE encapsulation to route captured traffic.

## Configure DSCP Marking on Egress GRE Tunnel in ERSPAN

### Configuration Example

This example shows how you can configure DSCP Marking on Egress GRE tunnel in ERSPAN.

```
Router#configure terminal
Router(config)#interface tunnel-ipl
Router(config-if)#tunnel tos 96
Router(config-if)#tunnel mode gre ipv4
Router(config-if)#tunnel source 192.0.2.1
Router(config-if)#tunnel destination 192.0.2.254
Router(config-if)#commit
```



**Note** You can configure DSCP value on both IPv4 and IPv6 headers.

## Running Configuration

```
interface tunnel-ip1
  tunnel tos 96
  tunnel mode gre ipv4
  tunnel source 192.0.2.1
  tunnel destination 192.0.2.254
!
```

## Verification

You can use the following commands to verify that ToS value is configured:

```
Router#show run interface tunnel-ip 1
interface tunnel-ip1
  ipv4 address 192.0.2.0/24
  tunnel tos 96
  tunnel mode gre ipv4
  tunnel source 192.0.2.1
  tunnel vrf red
  tunnel destination 192.0.2.254

Router#show monitor-session ERSPAN-2 status internal
Information from SPAN Manager and MA on all nodes:
Monitor-session ERSPAN-2 (ID 0x00000003) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip1 (0x20008024)
Last error: Success
Tunnel data:
  Mode: GREoIPv4
  Source IP: 192.0.2.1
  Dest IP: 192.0.2.254
  VRF: red
  VRF TBL ID: 0
  ToS: 96
  TTL: 255
  DFbit: Not set
```

## DSCP Bitmask to Filter Ingress ERSPAN Traffic

Table 23: Feature History Table

Feature Name	Release Information	Feature Description
DSCP Bitmask to Filter Ingress ERSPAN Traffic	Release 7.5.4	<p>You can now mirror multiple traffic flows for matched Differentiated Service Code Point (DSCP) value of IP header on the Encapsulated remote SPAN (ERSPAN). The matched DSCP value is based on the DSCP value and the bitmask configured in Access Control List (ACL) rule.</p> <p>Earlier, you could monitor single traffic flow by setting the <a href="#">RFC 4594</a> defined DSCP values in the GRE tunnel header.</p> <p>This feature introduces the following changes:</p> <ul style="list-style-type: none"> <li>• <b>CLI:</b> <code>deny (IPv4)</code>, <code>deny (IPv6)</code>, <code>permit (IPv4)</code>, and <code>permit (IPv6)</code> are modified to include new keyword <b>bitmask</b>.</li> <li>• <b>YANG DATA Model:</b> New XPaths for Cisco-IOS-XR-um-ipv4-access-list-cfg and Cisco-IOS-XR-um-ipv6-access-list-cfg (see <a href="#">Github</a>, <a href="#">YANG Data Models Navigator</a>).</li> </ul>

Starting Release 7.5.4, You can configure an ACL rule with DSCP bitmask on the ERSPAN GRE tunnels to mirror specific traffic flows.

Without ACL rule, ERSPAN mirrors all the traffic on the incoming port. When ACL is configured with DSCP and DSCP mask on the ERSPAN, ERSPAN mirrors the traffic whose DSCP value lies within the combination of DSCP value and the specified mask.

A DSCP value is mapped to a single traffic class as per the defined value in [RFC2474](#). Masking the DSCP value in ACL rule allows to mirror multiple traffic flows. DSCP value and mask operate similar to IPv4 address and mask.

### Configure DSCP Bitmask to Filter Ingress ERSPAN Traffic

To configure DSCP bitmask, use the `bitmask` option along with the `dscp` option while configuring the ACL.

#### Configuration Example for IPv4

This example shows how you can configure DSCP bitmask on ingress ERSPAN for IPv4 traffic.

```
/*configure the ACL*/
Router# config
Router(config)# ipv4 access-list acl1
Router(config-ipv4-acl)# 10 permit ipv4 host 192.0.2.1 any dscp af22 bitmask 0x3f
Router(config-ipv4-acl)# commit
Router(config-ipv4-acl)# exit

/* Perform the following configurations to attach the created ACL to an interface*/
Router(config)# interface HundredGigE0/0/0/6
Router(config-if)# ipv4 address 192.0.2.51 255.255.255.0
```

```
/* Monitor the ingress ACL applied and DSCP masked IPv4 traffic on ERSPAN*/
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv4 acl1
Router(config-if)# commit
```

### Running Configuration

```
Router(config)# show running-config ipv4 access-list
ipv4 access-list acl1
 10 permit ipv4 host 192.0.2.1 any dscp af22 bitmask 0x3f
!

interface HundredGigE0/0/0/6
 ipv4 address 192.0.2.51 255.255.255.0
 monitor-session TEST ethernet direction rx-only port-level acl ipv4 acl1
!
!
```

### Configuration Example for IPv6

This example shows how you can configure DSCP bitmask on ingress ERSPAN for IPv6 traffic.

```
/*configure the ACL*/
Router# config
Router(config)# ipv6 access-list acl1
Router(config-ipv6-acl)# 10 permit ipv6 host 2001:DB8::2/32 any dscp 33 bitmask 0x3f
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit

/* Perform the following configurations to attach the created ACL to an interface*/
Router(config)# interface HundredGigE 0/0/10/3
Router(config-if)# ipv6 address 2001:DB8::1/32

/* Monitor the ingress ACL applied and DSCP masked IPv4 traffic on ERSPAN*/
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv6 acl1
Router(config-if)# commit
```

### Running Configuration

```
Router(config)# show running-config ipv6 access-list
ipv6 access-list acl1
 10 permit ipv6 acl1 host 2001:DB8::2/32 any dscp 33 bitmask 0x3f
!

interface HundredGigE0/0/10/3
 ipv6 address 2001:db8::1/32
 monitor-session TEST ethernet direction rx-only port-level acl ipv6 acl1
!
!
```

# Monitor Multiple ERSPAN Sessions with SPAN and Security ACL

Table 24: Feature History Table

Feature Name	Release Information	Feature Description
Monitor Multiple ERSPAN Sessions with SPAN and Security ACL	Release 7.5.4	With this feature, you can use SPAN and security ACL together to monitor multiple ERSPAN sessions under the same source interface. SPAN ACL helps you to distribute the mirrored traffic over different destination interfaces and Security ACL helps you to allow selective incoming traffic.

Starting Cisco IOS XR Software Release 7.5.4 you can monitor multiple ERSPAN sessions using GREv4 and GREv6 under the same source interface. Multiple ERSPAN monitor sessions configured on an interface allow you to choose the destination interface for the mirrored traffic. For the configuration of monitor sessions, you can use SPAN and security ACLs together. The SPAN and security ACLs are applicable only in the ingress traffic.

## Configure Multiple Monitor ERSPAN Sessions with SPAN and Security ACL

This example shows how to configure SPAN and Security ACL for SPAN with GREv4 and GREv6 Monitor Sessions.

### Configuration example

Use the following configuration to attach SPAN and security ACLs for traffic mirroring.

```
Router# config
/*Perform the following configurations to attach the SPAN ACL to an interface*/
Router(config-if)#monitor-session always-on-v4 ethernet direction rx-only port-level
Router(config-if-mon)#acl ipv4 v4-monitor-acl1
Router(config-if-mon)#acl ipv6 v6-monitor-acl1
Router(config-if-mon)#exit
Router(config-if)#monitor-session on-demand-v4 ethernet direction rx-only port-level
Router(config-if-mon)#acl ipv4 v4-monitor-acl2
Router(config-if-mon)#acl ipv6 v6-monitor-acl2
Router(config-if-mon)#exit
/*Perform the following configurations to attach the security ACL to an interface*/
Router(config-if)#ipv4 access-group sec_aclv4 ingress
Router(config-if)#ipv6 access-group sec_aclv6 ingress
Router(config-if)#commit
```

### Running configuration

```
Router(config)#show running-config interface
monitor-session always-on-v4 ethernet direction rx-only port-level
```

```

acl ipv4 v4-monitor-acl2
acl ipv6 v6-monitor-acl2
!
monitor-session on-demand-v4 ethernet direction rx-only port-level
  acl ipv4 v4-monitor-acl2
  acl ipv6 v6-monitor-acl2
!
ipv4 access-group sec_aclv4 ingress
ipv6 access-group sec_aclv6 ingress
!
!

```

## SPAN to File

**Table 25: Feature History Table**

Feature Name	Release Information	Feature Description
SPAN to File Support for TX and RX	Release 7.5.3	<p>With this feature, the ability to capture the packet in TX direction along with the ability to store the capture on the file is supported.</p> <p>You can now capture the packet in the TX direction and store the capture on the file. Earlier, you could only capture or mirror the traffic in the RX direction. You now have the flexibility to choose TX, RX, or both directions.</p> <p>You can now capture and analyze the outgoing (TX) packets.</p>
Partial Packet Capture Ability for SPAN-to-File (RX)	Release 7.5.3	<p>With this feature, you can perform partial packet capture in the RX direction.</p> <p>Earlier, the ability for entire packet capture was available in the TX direction only, now you can choose entire or partial packet capture in the Rx direction also.</p> <p>Here, partial packet capture is also known as truncation.</p>
SPAN to File - PCAPng File Format	Release 7.3.1	<p>PCAPng is the next generation of packet capture format that contains a dump of data packets captured over a network and stored in a standard format.</p> <p>The PCAPng file contains different types of information blocks, such as the section header, interface description, enhanced packet, simple packet, name resolution, and interface statistics. These blocks can be used to rebuild the captured packets into recognizable data.</p> <p>The PCAPng file format:</p> <ul style="list-style-type: none"> <li>• Provides the capability to enhance and extend the existing capabilities of data storage over time</li> <li>• Allows you to merge or append data to an existing file.</li> <li>• Enables to read data independently from network, hardware, and operating system of the machine that made the capture.</li> </ul>

SPAN to File is an extension of the pre-existing SPAN feature that allows network packets to be mirrored to a file instead of an interface. This helps in the analysis of the packets at a later stage. The file format is PCAP, which helps that data to be used by tools, such as tcpdump or Wireshark.




---

**Note** A maximum of 100 source ports are supported across the system. Individual platforms may support lower numbers. All the SPAN sessions are configured under the Ethernet class. At any given time, the system supports four SPAN to File sessions.

---

When you configure a file as a destination for a SPAN session, the system creates buffer on each node to which the network packets are logged. The buffer is for all packets on the node regardless of which interface they are from. That is, multiple interfaces can provide packets to the same buffer. The system deletes the buffer when the session configuration is removed. Each node writes a file on the active RP, which contains the node ID of the node on which the buffer was located.

The minimum buffer size is 1KB. The maximum buffer size is 1000KB and default buffer size is 2KB.

If multiple interfaces are attached to a session, then interfaces on the same node are expected to have their packets sent to the same file. Bundle interfaces can be attached to a session with a file destination, which is similar to attaching individual interfaces.

From Cisco IOS XR Software Release 7.5.3 onwards, the capture of all the outgoing packets from the router is supported.

Earlier to Cisco IOS XR Software Release 7.5.3, there was no functionality which enables to capture the payload of packets coming from your customers for security reasons.

#### Limitations and Restrictions for SPAN to File

- Only incoming packet mirroring on the source interface is supported. Outgoing mirrored packets cannot be dumped to the file.

However, from Cisco IOS XR Software Release 7.5.3 onwards, there are no restrictions.

- SPAN ACLs can only be applied in ingress direction only. Hence, ACLs for SPAN to File can only be applied in ingress direction only.
- ACL on MPLS traffic is not supported.
- MPLS over GRE traffic is supported, however, GRE interfaces cannot be configured as source interfaces.
- Packet truncation applies for SPAN to File and ERSPAN interfaces only. If you change the destination to Local SPAN, then an **ios\_msg** is displayed as a warning. The entire packet is mirrored after this message is displayed.

**Example:** The Partial Packet Capture feature is not supported by Local SPAN. The entire Packet will be mirrored.

- Packet truncation is per monitor session.
- Currently, truncation per interface is not supported.
- For outgoing (TX) SPAN to File, Security ACL is not supported.
- For outgoing (TX) SPAN to File, only transit traffic is mirrored.

Self-originating traffic cannot be mirrored.



### Supported capabilities for SPAN to File

- The ability to mirror outgoing traffic and punt it to the CPU across all NPU versions.
- Ability to mirror outgoing IPv4, IPv6, and MPLS traffic to file.
- Ability to mirror outgoing traffic across all types of L3 interfaces, including physical, sub, bundle, and bundle sub interfaces
- Ability to mirror outgoing traffic across L2 or BVI interfaces.
- Ability to enable the new SPAN to File truncation configuration for both RX and TX direction. You can specify the `both` keyword to enable RX and TX mirroring on a single source interface.

See [Configuring SPAN to File for Truncation and Direction, on page 174](#)

- Ability to configure a different truncation size on each monitor session.
- Ability to configure SPAN to File mirroring packet truncation size from 1 to 10000. If you try to configure a value out of the range, the configuration will not accept it and displays an error message.
- Ability to change the truncation size, when packet collecting has stopped. Removing or re-adding the monitor session is not required.
- Ability to change the truncation size during packet collecting ON. Not required to stop the monitor session.
- The entire packet is mirrored by default, without the mirror first (truncation size) configuration.

Also, if the packet size is less than the configured truncation size, the entire packet is mirrored.

## Action Commands for SPAN to File

Action commands allows you to start and stop network packet collection. You can run the action commands on sessions where the destination is a file. The action command autocompletes names of the globally configured SPAN to File sessions. The following table provides more information on action commands.

**Table 26: Action Commands for SPAN to File**

Action	Command	Description
Start	<code>monitor-session &lt;name&gt;</code> <code>packet-collection start</code>	Use this command to start writing packets for the specified session to the configured buffer.

Action	Command	Description
Stop	<pre>monitor-session &lt;name&gt; packet-collection stop [ discard-data   write directory &lt;dir&gt; filename &lt;filename&gt; ]</pre>	<p>Use this command to stop writing packets to the configured buffer. If you specify the <code>discard-data</code> option, the system clears the buffer. Whereas if you specify the <code>write</code> option, the system writes the buffer to disk before clearing.</p> <p>When you must write buffer to disk, you must save the file in a <code>.pap</code> format at this location,  <code>/&lt;directory&gt;/&lt;node_id&gt;/&lt;filename&gt;.pcap</code>.  If you add a <code>.pcap</code> extension while specifying the filename, the system removes <code>.pcap</code> so that the extension is not added twice.</p>

## Configuring SPAN to File

Use the following command to configure SPAN to File:

```
monitor-session <name> [ethernet|ipv4|ipv6|mpls-ipv4|mpls-ipv6]
destination file [size <kbytes>] [buffer-type linear]
```

The `monitor-session <name> [ethernet|ipv4|ipv6|mpls-ipv4|mpls-ipv6]` part of the command creates a monitor-session with the specified name and class and is a pre-existing chain point from the current SPAN feature. The `destination file [size <kbytes>] [buffer-type linear]` part of the command adds a new “file” option to the existing “destination”.

`destination file` has the following configuration options:

- Buffer size.
- Two types of buffer:
  - Circular: Once the buffer is full, the start is overwritten.
  - Linear: Once the buffer is full, no further packets are logged.



**Note** The default buffer-type is circular. Only linear buffer is explicitly configurable. Changing any of the parameters (buffer size or type) recreates the session, and clears any buffers of packets.

All configuration options which are applied to an attachment currently supported for other SPAN types should also be supported by SPAN to file. This may include:

- ACLs
- Write only first X bytes of packet.
- In Cisco IOS XR Release 7.5.3, truncation per global session is supported and not per interface.



**Note** These options are implemented by the platform when punting the packet.

Once a session has been created, then interfaces may be attached to it using the following configuration:

```
interface GigabitEthernet 0/0/0/0
  monitor-session <name> [ethernet|ipv4|ipv6|mpls-ipv4|mpls-ipv6]
```

The attachment configuration is unchanged by SPAN to File feature.

### Configuration Examples

To configure a `mon1` monitor session, use the following commands:

```
monitor-session mon1 ethernet
  destination file size 230000
  !
```

In the above example, omitting the `buffer-type` option results in default circular buffer.

To configure a `mon2` monitor session, use the following commands:

```
monitor-session mon2 ethernet
  destination file size 1000 buffer-type linear
  !
```

To attach monitor session to a physical or bundle interface, use the following commands:

```
RP/0/RSP0/CPU0:router#show run interface Bundle-Ether 1
Fri Apr 24 12:12:59.348 EDT
interface Bundle-Ether1
monitor-session ms7 ethernet|ipv4|ipv6|mpls-ipv4|mpls-ipv6]
[direction {rx-only|tx-only|both[SW(1) ]}] [port-level]
acl [<acl_name>]!
```

### Running Configuration

```
!! IOS XR Configuration 7.1.1.124I
!! Last configuration change at Tue Nov 26 19:29:05 2019 by root
!
hostname OC
logging console informational
!
monitor-session mon1 ethernet
  destination file size 230000 buffer-type circular
!
monitor-session mon2 ethernet
  destination file size 1000 buffer-type linear
!
interface Bundle-Ether1
monitor-session ms7 ethernet
  direction rx-only
end
```

### Verification

To verify packet collection status:

```
RP/0/RP0/CPU0:router#show monitor-session status
Monitor-session mon1
Destination File - Packet collecting
=====
Source Interface      Dir.      Status
-----
```

```
Hu0/9/0/2                Rx          Operational
```

```
Monitor-session mon2
Destination File - Packet collecting
=====
Source Interface          Dir      Status
-----
BE2.1.                    Rx      Operational
```

If packet collection is not active, the following line is displayed:

```
Monitor-session mon2
Destination File - Not collecting
```

## Configuring SPAN to File for Truncation and Direction

### Configuring SPAN to File for Truncation

Use the **mirror first** command in monitor session configuration mode to create a SPAN to File monitor session for mirroring the packets with truncation enabled:

```
monitor-session <name> [ethernet]
destination file [size <kbytes>] [buffer-type linear|circular]
mirror first <number>
```

Once a session has been created, then interfaces may be attached to it using the following configuration:

```
interface <>
  monitor-session session-name ethernet direction rx-only|tx-only|both | acl [acl_name]
```

### Configuration Examples

To configure a `mon1` monitor session, use the following commands:

```
monitor-session mon1 ethernet
  destination file
  mirror first 128
!
```

### Configuring SPAN to File for Direction

Use the following command to create a SPAN to File monitor session for mirroring the packets:

```
monitor-session mon2 ethernet
  destination file
!
```

Attach the session which has been created to the interfaces using the following configuration:

```
interface <>
  monitor-session session-name ethernet direction rx-only|tx-only|
acl [acl_name]
```

### Running Configuration for all

```
monitor-session mon3 ethernet
  destination file
!

interface Hu0/9/0/2
  monitor-session mon1 ethernet
  direction rx-only
!
```

```

interface bundle-ether1
monitor-session mon2 ethernet
direction tx-only
!

interface bundle-ether2.1
monitor-session mon3 ethernet
direction both
end

```

### Verification

The `show monitor-session status` displays the direction.

```

Router#show monitor-session status
Monitor-session mon1
Destination File - Packet collecting
=====
Source Interface      Dir      Status
-----
Hu0/9/0/2             Rx       Operational
Monitor-session mon2
Destination File - Packet collecting
=====
Source Interface      Dir      Status
-----
BE1                   Tx       Operational
Monitor-session mon3
Destination File - Packet collecting
=====
Source Interface      Dir      Status
-----
BE2.1                 Both    Operational

```

## Mirroring Forward-Drop Packets

Table 27: Feature History Table

Feature Name	Release Information	Description
Mirroring Forward-Drop Packets	Release 7.5.4	<p>Mirroring forward-drop packets feature copies or mirrors the packets that are dropped during the forwarding process at the router ingress to a configured destination. These mirrored packets can be captured and analyzed using network monitoring tools. The analysis of dropped packets helps you understand the types of traffic that are blocked, analyze potential security threats, troubleshoot, and optimize network performance.</p> <p>This feature introduces the following changes:</p> <ul style="list-style-type: none"> <li>• <b>CLI:</b> <code>forward-drop rx</code></li> <li>• <b>YANG Data Model:</b> New XPath for Cisco-IOS-XR-um-monitor-session-cfg.yang (see <a href="#">GitHub</a>, <a href="#">YANG Data Models Navigator</a>)</li> </ul>

In a network, packets are forwarded from one device to another until they reach their destination. However, in some cases, routers may drop packets during this forwarding process. These packets are known as forward-drop packets.

The packet drop can happen for several reasons, such as congestion on the network, errors in the packet header or payload, blocking by firewall or access control lists (ACL), and so on. These forward-drop packets are typically discarded before they can reach their intended destination, and may have to be re-transmitted by the source device. This feature supports mirroring of these forward-drop packets at the ingress (Rx direction) to another destination. When a global forward-drop session is configured for the router, the forward-drop packets at the ingress are mirrored or copied to the configured destination. You can configure the mirror destination as a file (for SPAN-to-file sessions) or an IPv4 GRE tunnel ID (for ERSPAN).

Mirroring forward-drop packets to a suitable destination for analysis can help in the following:

- **Network visibility:** By mirroring and analyzing forward-drop packets, network administrators gain better visibility into the types of traffic that are blocked by the firewalls and access control lists (ACL).
- **Threat detection:** As the original dropped packet is forwarded without any change, it helps in identifying the source of potential security threats.
- **Troubleshooting:** Analyzing forward-drop packets helps in troubleshooting network issues that may be causing the packet drop. This helps in taking proactive measures to avoid escalation of the issue.

#### Guidelines and Restrictions

- Only one global forward-drop session can be configured on a router.
- When traffic-class is configured under monitor-session for forward-drop, the type of service (ToS) byte of the outgoing ERSPAN packet is overwritten with the configured traffic-class value.
- In-band traffic destined to router management interface cannot be captured using this functionality.

## Configuring Forward-Drop

Perform the following tasks on the router to configure a global session for mirroring forward-drop packets:

1. Configure the tunnel mode.
2. Configure the tunnel source.
3. Configure the tunnel destination.
4. Configure a traffic mirroring session.
5. Associate a destination interface with the traffic mirroring session.
6. Run **forward-drop rx** command to start mirroring forward-drop packets.

This example shows how to configure a global traffic mirroring session for forward-drop packets.

```
Router(config)# interface tunnel-ip 2
Router(config-if)# tunnel mode gre ipv4
Router(config-if)# tunnel source 20.20.20.20
Router(config-if)# tunnel destination 192.1.1.3
Router(config-if) !
Router(config)# monitor-session mon2 ethernet
Router(config)#destination interface tunnel-ip2
```

```
Router(config)#forward-drop rx
Router(config)#!
```

### Running Configuration

This section shows forward-drop running configuration.

```
RP/0/RSP0/CPU0:router#sh running-config
interface tunnel-ip 2
 tunnel mode gre ipv4
 tunnel source 20.20.20.20
 tunnel destination 192.1.1.3
 !
 monitor-session mon2 ethernet
 destination interface tunnel-ip2
 forward-drop rx
 !
```

### Verification

Verify the forward-drop packets are mirrored using the **show monitor-session** command.

```
Router#show monitor-session mon2 status detail
Mon Aug 15 19:14:31.975 UTC
Monitor-session mon2
  Destination interface tunnel-ip2
  All forwarding drops:
    Direction: Rx
  Source Interfaces
  -----
```

## Traffic Mirroring Configuration Examples

This section contains examples of how to configure traffic mirroring:

### Viewing Monitor Session Status: Example

This example shows sample output of the **show monitor-session** command with the **status** keyword:

```
RP/0/RP0/CPU0:router# show monitor-session status

Monitor-session cisco-rtp1
Destination interface HundredGigE0/5/0/38
=====
Source Interface   Dir   Status
-----
Gi0/5/0/4         Rx   Operational
Gi0/5/0/17        Rx   Operational

RP/0/RP0/CPU0:router# show monitor-session status detail

Monitor-session sess1
Destination interface is not configured
Source Interfaces
-----
HundredGigE0/0/0/0
  Direction: Rx
  ACL match: Enabled
```

```

Portion: Full packet
Status: Not operational (destination interface not known).
HundredGigE0/0/0/2
Direction: Rx
ACL match: Disabled
Portion: First 100 bytes

```

```
RP/0/RP0/CPU0:router# show monitor-session status error
```

```

Monitor-session ms1
Destination interface HundredGigE0/2/0/15 is not configured
=====
Source Interface   Dir   Status
-----
Monitor-session ms2
Destination interface is not configured
=====
Source Interface   Dir   Status
-----

```

## Monitor Session Statistics: Example

The monitor session statistics is provided in the form of packets and bytes. Use the following command to get the status:

```

RP/0/RP0/CPU0:router# show monitor-session <session_name> status internal
RP/0/RP0/CPU0:Router1#show monitor-session mon2 status internal
Wed Oct  9 19:39:30.402 UTC
Information from SPAN Manager and MA on all nodes:
Monitor-session mon2 (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip2 (0x0f000034)
Last error: Success
Tunnel data:
  Mode: GREoIPv4
  Source IP: 2.2.2.2
  Dest IP: 130.1.1.2
  VRF:
  ToS: 0 (copied)
  TTL: 255
  DFbit: Not set
0/1/CPU0: Destination interface tunnel-ip2 (0x0f000034)
Tunnel data:
  Mode: GREoIPv4
  Source IP: 2.2.2.2
  Dest IP: 130.1.1.2
  VRF:
  ToS: 0 (copied)
  TTL: 255
  DFbit: Not set

Information from SPAN EA on all nodes:
Monitor-session 0x00000001 (Ethernet)
0/1/CPU0: Name 'mon2', destination interface tunnel-ip2 (0x0f000034)
Platform, 0/1/CPU0:

Monitor Session ID: 1

Monitor Session Packets: 11
Monitor Session Bytes: 1764

```



```

0/2/CPU0: Name 'mon2', destination interface tunnel-ip2 (0x0f000034)
Platform, 0/2/CPU0:

Monitor Session ID: 1

Monitor Session Packets: 0
Monitor Session Bytes: 0

```

**Note**

- Currently, the system does not allow you to clear these counters.
- The counters are present on the line-card that contains the interface over which the mirrored packets are sent to the ERSPAN session destination.

If required, to clear the counters, delete and recreate the monitor session. Also, clear the counters by performing a Shut/No Shut of the tunnel interface, which triggers a Delete+Create action.

## Layer 3 ACL-Based Traffic Mirroring: Example

This example shows how to configure Layer 3 ACL-based traffic mirroring:

```

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# monitor-session ms1
RP/0/RP0/CPU0:router(config-mon)# destination tunnel-ip 1

RP/0/RP0/CPU0:router(config-mon)# commit

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface HundredGigE/2/0/11
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group span ingress
RP/0/RP0/CPU0:router(config-if)# monitor-session ms1 ethernet direction rx-only acl
RP/0/RP0/CPU0:router(config-if-mon)# commit

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 access-list span
RP/0/RP0/CPU0:router(config-ipv4-acl)# 5 permit ipv4 any any dscp 5 capture
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 any any
RP/0/RP0/CPU0:router(config-ipv4-acl)# commit

```

## Troubleshooting Traffic Mirroring

When you encounter any issue with traffic mirroring, begin troubleshooting by checking the output of the **show monitor-session status** command. This command displays the recorded state of all sessions and source interfaces:

```

Monitor-session sess1
<Session status>
=====
Source Interface   Dir   Status
-----
Gi0/0/0/0         Both <Source interface status>
Gi0/0/0/2         Both <Source interface status>

```

In the preceding example, the line marked as `<Session status>` can indicate one of these configuration errors:

Session Status	Explanation
Session is not configured globally	The session does not exist in global configuration. Check <b>show run</b> command output to ensure that a session with a correct name has been configured.
Destination interface <code>&lt;intf&gt;</code> is not configured	The interface that has been configured as the destination does not exist. For example, the destination interface may be configured to be a VLAN subinterface, but the VLAN subinterface may not have been yet created.
Destination interface <code>&lt;intf&gt;</code> ( <code>&lt;down-state&gt;</code> )	The destination interface is not in Up state in the Interface Manager. You can verify the state using the <b>show interfaces</b> command. Check the configuration to see what might be keeping the interface from coming up (for example, a sub-interface needs to have an appropriate encapsulation configured).

The `<Source interface status>` can report these messages:

Source Interface Status	Explanation
Operational	Everything appears to be working correctly in traffic mirroring PI. Please follow up with the platform teams in the first instance, if mirroring is not operating as expected.
Not operational (Session is not configured globally)	The session does not exist in global configuration. Check the <b>show run</b> command output to ensure that a session with the right name has been configured.
Not operational (destination interface not known)	The session exists, but it either does not have a destination interface specified, or the destination interface named for the session does not exist (for example, if the destination is a sub-interface that has not been created).
Not operational (source same as destination)	The session exists, but the destination and source are the same interface, so traffic mirroring does not work.
Not operational (destination not active)	The destination interface or pseudowire is not in the Up state. See the corresponding <i>Session status</i> error messages for suggested resolution.
Not operational (source state <code>&lt;down-state&gt;</code> )	The source interface is not in the Up state. You can verify the state using the <b>show interfaces</b> command. Check the configuration to see what might be keeping the interface from coming up (for example, a sub-interface needs to have an appropriate encapsulation configured).

Source Interface Status	Explanation
Error: see detailed output for explanation	Traffic mirroring has encountered an error. Run the <b>show monitor-session status detail</b> command to display more information.

The **show monitor-session status detail** command displays full details of the configuration parameters, and of any errors encountered. For example:

```
RP/0/RP0/CPU: router#show monitor-session status detail
```

```
Monitor-session sess1
Destination interface is not configured
Source Interfaces
-----
HundredGigE0/0/0/0
  Direction: Both
  ACL match: Enabled
  Portion: Full packet
  Status: Not operational (destination interface not known)
HundredGigE0/0/0/2
  Direction: Both
  ACL match: Disabled
  Portion: First 100 bytes
  Status: Not operational (destination interface not known). Error: 'Viking SPAN PD' detected
the 'warning' condition 'PRM connection creation failure'.
Monitor-session foo
Destination next-hop HundredGigE 0/0/0/0
Source Interfaces
-----
HundredGigE 0/1/0/0.100:
  Direction: Both
  Status: Operating
HundredGigE 0/2/0/0.200:
  Direction: Tx
  Status: Error: <blah>

Monitor session bar
No destination configured
Source Interfaces
-----
HundredGigE 0/3/0/0.100:
  Direction: Rx
  Status: Not operational(no destination)
```

### Additional Debugging Commands

Here are additional trace and debug commands:

```
RP/0/RP0/CPU0:router# show monitor-session platform trace ?
```

```
all    Turn on all the trace
errors Display errors
events Display interesting events
```

```
RP/0/RP0/CPU0:router# show monitor-session trace ?
```

```
process Filter debug by process
```

```

RP/0/RP0/CPU0:router# debug monitor-session platform ?

all    Turn on all the debugs
errors VKG SPAN EA errors
event  VKG SPAN EA event
info   VKG SPAN EA info

RP/0/RP0/CPU0:router# debug monitor-session platform all

RP/0/RP0/CPU0:router# debug monitor-session platform event

RP/0/RP0/CPU0:router# debug monitor-session platform info

RP/0/RP0/CPU0:router# show monitor-session status ?

detail Display detailed output
errors  Display only attachments which have errors
internal Display internal monitor-session information
|       Output Modifiers

RP/0/RP0/CPU0:router# show monitor-session status

RP/0/RP0/CPU0:router# show monitor-session status errors

RP/0/RP0/CPU0:router# show monitor-session status internal

```

If there is no route to the destination IPv4 address, the status displayed for the monitor session looks like this:

```

RP/0/RP0/CPU0:Router1#show monitor-session mon2 status internal
Wed Oct  9 19:24:06.084 UTC
Information from SPAN Manager and MA on all nodes:
Monitor-session mon2 (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip2 (0x0f000034) (down)
          Last error: Success
          Tunnel data:
            Mode: GREoIPv4
            Source IP: 2.2.2.2
            Dest IP: 130.10.10.2
            VRF:
            ToS: 0 (copied)
            TTL: 255
            DFbit: Not set
0/1/CPU0: Destination interface is not configured
          Tunnel data:
            Mode: GREoIPv4
            Source IP: 2.2.2.2
            Dest IP: 130.10.10.2
            VRF:
            ToS: 0 (copied)
            TTL: 255
            DFbit: Not set

```

To verify if there is a route to the destination IPv4 address, use the following command:

```

RP/0/RP0/CPU0:Router1#show cef ipv4 130.10.10.2
Wed Oct  9 19:25:12.282 UTC
0.0.0.0/0, version 0, proxy default, default route handler, drop adjacency, internal 0x1001011
 0x0 (ptr 0x8e88d2b8) [1], 0x0 (0x8ea4d0a8), 0x0 (0x0)
Updated Oct  9 19:03:36.068
Prefix Len 0, traffic index 0, precedence n/a, priority 15
  via 0.0.0.0/32, 3 dependencies, weight 0, class 0 [flags 0x0]
  path-idx 0 NHID 0x0 [0x8e2db240 0x0]
  next hop 0.0.0.0/32
  drop adjacency

```

When a route is present, the command used in the previous example displays the following:

```
RP/0/RP0/CPU0:Router1#show cef ipv4 130.10.10.2
Wed Oct 9 19:26:06.141 UTC
130.1.1.0/24, version 20, internal 0x1000001 0x0 (ptr 0x8e88aa18) [1], 0x0 (0x8ea4dc68),
0x0 (0x0)
Updated Oct 9 19:26:02.139
Prefix Len 24, traffic index 0, precedence n/a, priority 3
  via 131.1.1.1/32, HundredGigE0/1/0/2, 2 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0x8f8e2260 0x0]
    next hop 131.10.10.1/32
    local adjacency
```

The show monitor command displays the following:

```
show monitor-session mon2 status internal
Wed Oct 9 19:26:12.405 UTC
Information from SPAN Manager and MA on all nodes:
Monitor-session mon2 (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip2 (0x0f000034)
Last error: Success
Tunnel data:
  Mode: GREoIPv4
  Source IP: 2.2.2.2
  Dest IP: 130.10.10.2
  VRF:
  ToS: 0 (copied)
  TTL: 255
  DFbit: Not set
0/1/CPU0: Destination interface tunnel-ip2 (0x0f000034)
Tunnel data:
  Mode: GREoIPv4
  Source IP: 2.2.2.2
  Dest IP: 130.10.10.2
  VRF:
  ToS: 0 (copied)
  TTL: 255
  DFbit: Not set

Information from SPAN EA on all nodes:
Monitor-session 0x00000001 (Ethernet)
0/1/CPU0: Name 'mon2', destination interface tunnel-ip2 (0x0f000034)
Platform, 0/1/CPU0:

  Monitor Session ID: 1

  Monitor Session Packets: 0
  Monitor Session Bytes: 0

0/2/CPU0: Name 'mon2', destination interface tunnel-ip2 (0x0f000034)
Platform, 0/2/CPU0:

  Monitor Session ID: 1

  Monitor Session Packets: 0
  Monitor Session Bytes: 0

Missing ARP to the next hop to the destination
This condition is detected via this show command:
show monitor-session mon2 status internal
```

After resolving ARP for the next hop, which is done by invoking a ping command to the destination, the show command output displays the following:

```

RP/0/RP0/CPU0:Router1#show monitor-session mon2 status internal
Wed Oct  9 19:32:24.856 UTC
Information from SPAN Manager and MA on all nodes:
Monitor-session mon2 (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip2 (0x0f000034)
      Last error: Success
      Tunnel data:
        Mode: GREoIPv4
        Source IP: 2.2.2.2
        Dest IP: 130.10.10.2
        VRF:
        ToS: 0 (copied)
        TTL: 255
        DFbit: Not set
0/1/CPU0: Destination interface tunnel-ip2 (0x0f000034)
      Tunnel data:
        Mode: GREoIPv4
        Source IP: 2.2.2.2
        Dest IP: 130.10.10.2
        VRF:
        ToS: 0 (copied)
        TTL: 255
        DFbit: Not set

Information from SPAN EA on all nodes:
Monitor-session 0x00000001 (Ethernet)
0/1/CPU0: Name 'mon2', destination interface tunnel-ip2 (0x0f000034)
Platform, 0/1/CPU0:

  Monitor Session ID: 1
    Monitor Session Packets: 0
    Monitor Session Bytes: 0

0/2/CPU0: Name 'mon2', destination interface tunnel-ip2 (0x0f000034)
Platform, 0/2/CPU0:

  Monitor Session ID: 1
    Monitor Session Packets: 0
    Monitor Session Bytes: 0

```

### Where to Go Next

When you have configured an Ethernet interface, you can configure individual VLAN subinterfaces on that Ethernet interface.

For information about modifying Ethernet management interfaces for the shelf controller (SC), route processor (RP), and distributed RP, see the Advanced Configuration and Modification of the Management Ethernet Interface later in this document.

For information about IPv6 see the Implementing Access Lists and Prefix Lists on

Cisco IOS XR Software module in the Cisco IOS XR IP Addresses and Services Configuration Guide.



## CHAPTER 9

# Configuring Virtual Loopback and Null Interfaces

This module describes the configuration of loopback and null interfaces. Loopback and null interfaces are considered virtual interfaces.

A virtual interface represents a logical packet switching entity within the router. Virtual interfaces have a global scope and do not have an associated location. Virtual interfaces have instead a globally unique numerical ID after their names. Examples are Loopback 0, Loopback 1, and Loopback 99999. The ID is unique per virtual interface type to make the entire name string unique such that you can have both Loopback 0 and Null 0.

Loopback and null interfaces have their control plane presence on the active route switch processor (RP). The configuration and control plane are mirrored onto the standby RP and, in the event of a failover, the virtual interfaces move to the ex-standby, which then becomes the newly active RP.

### Feature History for Configuring Loopback and Null Interfaces on Cisco IOS XR Software

Release	Modification
Release 7.0.11	This feature was introduced.

- [Prerequisites for Configuring Virtual Interfaces, on page 185](#)
- [Information About Configuring Virtual Interfaces, on page 185](#)
- [How to Configure Virtual Interfaces, on page 187](#)
- [Configuration Examples for Virtual Interfaces, on page 189](#)

## Prerequisites for Configuring Virtual Interfaces

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs that you need for each command. If you suspect a user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

## Information About Configuring Virtual Interfaces

To configure virtual interfaces, you must understand the following concepts:

## Virtual Loopback Interface Overview

A virtual loopback interface is a virtual interface with a single endpoint that is always up or active. Any packet that the system transmits over a virtual loopback interface is immediately received by the same interface. Loopback interfaces emulate a physical interface.

In Cisco IOS XR Software, virtual loopback interfaces perform these functions:

- Loopback interfaces can act as a termination address for routing protocol sessions. This allows routing protocol sessions to stay up even if the outbound interface is down.
- You can ping the loopback interface to verify that the router IP stack is working properly.

In applications where other routers or access servers attempt to reach a virtual loopback interface, you must configure a routing protocol to distribute the subnet assigned to the loopback address.

Packets routed to the loopback interface are rerouted back to the router or access server, and processed locally. IP packets routed out to the loopback interface but not destined to the loopback interface are dropped. Under these two conditions, the loopback interface can behave like a null interface.

## Null Interface Overview

A null interface functions similarly to the null devices available on most operating systems. This interface is always up and can never forward or receive traffic; encapsulation always fails. The null interface provides an alternative method of filtering traffic. You can avoid the overhead that is involved with using access lists by directing undesired network traffic to the null interface.

The only interface configuration command that you can specify for the null interface is the **ipv4 unreachable** command. With the **ipv4 unreachable** command, if the software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an Internet Control Message Protocol (ICMP) protocol unreachable message to the source. If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message. By default, the system enables the **ipv4 unreachable** command. If we do not want ICMP to send protocol unreachable, then you need to configure using the **ipv4 icmp unreachable disable** command.

By default, the system creates the Null 0 interface during boot process and you cannot remove it. You can configure the **ipv4 unreachable** command for this interface, but most configuration is unnecessary because this interface just discards all the packets that the system sends.

Use the **show interfaces null0** command to display the Null 0 interface.

## Virtual Management Interface Overview

Configuring an IPv4 virtual address enables you to access the router from a single virtual address with a management network without prior knowledge of which RP is active. An IPv4 virtual address persists across route switch processor (RP) failover situations. For this to happen, the virtual IPv4 address must share a common IPv4 subnet with a management Ethernet interface on both the RPs.

On a router where each RP has multiple management Ethernet interfaces, the virtual IPv4 address maps to the management Ethernet interface on the active RP that shares the same IP subnet.



## Active and Standby RPs and Virtual Interface Configuration

The standby RP is available and in a state in which it can take over the work from the active RPs should that prove necessary. Conditions that necessitate the standby RP to become the active RP and assume the active RP's duties include:

- Failure detection by a watchdog
- Administrative command to take over
- Removal of the active RP from the chassis

If a second RP is not present in the chassis while the first is in operation, a second RP may be inserted and automatically becomes the standby RP. The standby RP may also be removed from the chassis with no effect on the system other than loss of RP redundancy.

After failover, the virtual interfaces all are present on the standby (now active) RP. Their state and configuration are unchanged and there has been no loss of forwarding (in the case of tunnels) over the interfaces during the failover. The routers use nonstop forwarding (NSF) over bundles and tunnels through the failover of the host RP.



---

**Note** The user need not configure anything to guarantee that the standby interface configurations are maintained. Protocol configuration such as tacacs source-interface, snmp-server trap-source, ntp source, logging source-interface do not use the virtual management IP address as their source by default. Use the **ipv4 virtual address use-as-src-addr** command to ensure that the protocol uses the virtual IPv4 address as its source address. Alternatively, you can also configure a loopback address with the designated or desired IPv4 address and set that as the source for protocols such as TACACS+ using the **tacacs source-interface** command.

---

## How to Configure Virtual Interfaces

This section contains the following procedures:

### Configuring Virtual Loopback Interfaces

This task explains how to configure a basic loopback interface.

#### Restrictions

- The IP address of a loopback interface must be unique across all routers on the network.
- That IP address must not be used by another interface on the router.
- The IP address must not be used by an interface on any other router on the network.

```
RP/0/RP0/CPU0:router# configure
/* Enters interface configuration mode and names the new loopback interface */
RP/0/RP0/CPU0:router#(config)# interface Loopback 3
/* Assigns an IP address and subnet mask to the virtual loopback interface */
```

```
RP/0/RP0/CPU0:router(config-if)# ipv4 address 172.18.189.38/32

RP/0/RP0/CPU0:router(config-if)# end
RP/0/RP0/CPU0:router(config-if)# commit
```

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

```
/* Display the configuration of the loopback interface */
RP/0/RP0/CPU0:router# show interfaces Loopback 3
```

## Configuring Null Interfaces

This task explains how to configure a basic null interface.

```
/* Enters global configuration mode. */

RP/0/RP0/CPU0:router# configure

/* Enter the null 0 interface configuration mode. */

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

/* Save configuration changes. */

RP/0/RP0/CPU0:router(config-null0)# end

/* Verif the configuration of the null interface. */

RP/0/RP0/CPU0:router# show interfaces null 0
```

## Configuring Virtual IPv4 Interfaces

This task explains how to configure an IPv4 virtual interface.

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

/* Define an IPv4 virtual address for the management Ethernet interface. */
```

```
RP/0/RSP0/CPU0:router(config)# ipv4 virtual address 10.3.32.154/8
RP/0/RSP0/CPU0:router(config-null0)# end
or
RP/0/RSP0/CPU0:router(config-null0)# commit
```

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before
exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

This is an example for configuring a virtual IPv4 interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ipv4 virtual address 10.3.32.154/8
RP/0/RSP0/CPU0:router(config-null0)# commit
```

## Configuration Examples for Virtual Interfaces

This section provides the following configuration examples:

### Configuring a Loopback Interface: Example

The following example indicates how to configure a loopback interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface Loopback 3
RP/0/RP0/CPU0:router(config-if)# ipv4 address 172.18.189.38/32
RP/0/RP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes
RP/0/RP0/CPU0:router# show interfaces Loopback 3
```

```
Loopback3 is up, line protocol is up
Hardware is Loopback interface(s)
Internet address is 172.18.189.38/32
MTU 1514 bytes, BW Unknown
  reliability 0/255, txload Unknown, rxload Unknown
Encapsulation Loopback, loopback not set
Last clearing of "show interface" counters never
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 total input drops
```

```

0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 0 multicast packets
0 packets output, 0 bytes, 0 total output drops
Output 0 broadcast packets, 0 multicast packets

```

## Configuring a Null Interface: Example

The following example indicates how to configure a null interface:

```

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface Null 0
RP/0/RP0/CPU0:router(config-null0)# ipv4 unreachable
RP/0/RP0/CPU0:router(config-null0)# end
Uncommitted changes found, commit them? [yes]: yes
RP/0/RP0/CPU0:router# show interfaces Null 0

```

```

Null0 is up, line protocol is up
Hardware is Null interface
Internet address is Unknown
MTU 1500 bytes, BW Unknown
  reliability 0/255, txload Unknown, rxload Unknown
Encapsulation Null, loopback not set
Last clearing of "show interface" counters never
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 total input drops
  0 drops for unrecognized upper-level protocol
  Received 0 broadcast packets, 0 multicast packets
  0 packets output, 0 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets

```

## Configuring a Virtual IPv4 Interface: Example

```

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 virtual address 10.3.32.154/8
RP/0/RP0/CPU0:router(config-null0)# commit

```



# CHAPTER 10

## Configure GRE Tunnels

Tunneling provides a mechanism to transport packets of one protocol within another protocol. This chapter describes GRE tunneling protocol.

Release	Feature(s) Added
Release 7.3.1	GRE Tunnel feature was introduced.

- [GRE Tunnels](#), on page 191
- [Unidirectional GRE Encapsulation \(GREv4\)](#), on page 196
- [Unidirectional GRE Decapsulation \(GREv4\)](#), on page 196
- [ECMP and LAG Hashing for NVGRE Flows](#), on page 198

## GRE Tunnels

*Table 28: Feature History Table*

Feature Name	Release Information	Description
Disabling time-to-live (TTL) decrement at GRE encapsulation	Release 7.3.2	<p>This feature allows you to disable the time-to-live (TTL) decrement of the incoming packets. The result is that encapsulation of the original incoming packet takes place without any change in the TTL value.</p> <p>This feature avoids dropping incoming packets with a TTL value equal to one after GRE encapsulation.</p> <p>Before this release, the TTL value of incoming packets was decremented by one before GRE decapsulation.</p> <p>This feature introduces the <b>tunnel ttl disable</b> command.</p>

Feature Name	Release Information	Description
GRE Tunnel	Release 7.3.1	<p>Generic Routing Encapsulation (GRE) provides a simple approach to transporting packets of one protocol over another protocol using encapsulation. This capability is now extended to the Cisco 8000 Series Routers.</p> <p>This feature supports:</p> <ul style="list-style-type: none"> <li>• Unidirectional GRE encapsulation</li> <li>• Unidirectional GRE decapsulation</li> </ul> <p>And introduces the following commands:</p> <ul style="list-style-type: none"> <li>• <b>show interface tunnel accounting (encap)</b></li> <li>• <b>show interface tunnel accounting (decap)</b></li> </ul>
Outer-header hashing support for MPLSoGRE and IPoGRE traffic	Release 7.3.1	<p>This feature allows load-balancing of GRE traffic in transit routers. A transit node distributes incoming GRE traffic evenly across all available ECMP links in a GRE tunnel topology. A hashing function uses GRE outer and inner header tuples such as source IP, destination IP, protocol, and router ID to determine traffic entropy. This capability is now extended to the Cisco 8000 Series Routers.</p>

Generic Routing Encapsulation (GRE) is a tunneling protocol that provides a simple generic approach to transport packets of one protocol over another protocol by means of encapsulation. GRE encapsulates a payload, that is, an inner packet that should be delivered to a destination network inside an outer IP packet. The GRE tunnel behaves as virtual point-to-point link that has two endpoints identified by the tunnel source and tunnel destination address. The tunnel endpoints send payloads through GRE tunnels by routing encapsulated packets through intervening IP networks. Other IP routers along the way do not parse the payload (the inner packet); they only parse the outer IP packet as they forward it toward the GRE tunnel endpoint. Upon reaching the tunnel endpoint, GRE encapsulation is removed and the payload is forwarded to the packet's ultimate destination.

A tunnel configured using encapsulation mode performs encapsulation of IPv4/IPv6 payload inside the GRE header. A tunnel configured using decapsulation mode performs the opposite. Here, outer GRE header is decapsulated and the inner IPv4/IPv6/MPLS payload is forwarded to the next hop router. Both encapsulation and decapsulation tunnel interfaces collect statistics periodically. The statistics can be displayed on demand using the CLI commands `show interface tunnel-ipl accounting` and `show policy-map type pbr address-family ipv4 statistics`. For more information, see [Unidirectional GRE Encapsulation \(GREv4\)](#), on page 196 and [Unidirectional GRE Decapsulation \(GREv4\)](#), on page 196.

To perform load-balancing of GRE traffic in transit routers, a transit node distributes incoming GRE traffic evenly across all available ECMP links in a GRE tunnel topology. Furthermore, to determine traffic entropy, a hashing function uses GRE outer and inner header tuples such as source IP, destination IP, protocol, and router ID.

## GRE Encapsulation and Decapsulation Over BVI

Table 29: Feature History Table

Feature Name	Release Information	Description
GRE Encapsulation and Decapsulation Over BVI	Release 7.5.4	<p>You can now transport packets using the GRE protocol over Bridge-Group Virtual Interfaces (BVI).</p> <p>This feature uses GRE to encapsulate packets between two endpoints and transmit the encapsulated packets over a BVI interface. At the destination, the GRE packet is decapsulated.</p> <p>GRE encapsulation and decapsulation over BVI allows transmitting packets securely using network layer protocols while maintaining Layer 2 connectivity between the physical interfaces.</p>

From Cisco IOS XR Release 7.5.4, GRE packets are supported over a BVI interface. This support provides GRE encapsulation and decapsulation over the BVI interfaces.

The BVI is a virtual interface within the router that acts like a normal routed interface. The BVI does not support bridging itself, but acts as a gateway for the corresponding bridge-domain to a routed interface within the router. A BVI is associated with a single bridge domain and represents the link between the bridging and the routing domains on the router.

When using GRE over BVI, the GRE header is added to the original IP packet before it is sent to the BVI. The BVI then bridges the encapsulated packet to the destination interface, which is a BVI, physical interface, or a remote network.

When the encapsulated packet reaches its destination, the receiving interface performs GRE decapsulation, which involves removing the GRE header from the original IP packet. The resulting IP packet is then forwarded to its final destination.

For information on BVI, see the *Integrated Routing and Bridging* section in the *L2VPN Configuration Guide for Cisco 8000 Series Routers*.

## Supported Features on a GRE Tunnel

GRE tunnel supports the following features:

- GRE or IP-in-IP tunnels support 16 unique source addresses. These 16 unique source addresses are repeated multiple times to configure 1000 encapsulation tunnels or 64 decapsulation tunnels.
- GRE encapsulation supports the following features:
  - IPv4/IPv6 over GRE IPv4 transport
  - MPLS PoP over GRE IPv4 transport
  - ABF (Access List Based Forwarding) v4/v6 over GRE
  - VRF (Virtual Routing and Forwarding) support over GRE
- GRE decapsulation supports the following features:
  - PBR-based GRE decapsulation configuration

- CLI-based GRE decapsulation configuration
- IPv4/IPv6 over GRE decapsulation
- MPLS/SRTE over GRE decapsulation
- A GRE tunnel in decapsulation mode has only tunnel source configured, without any tunnel destination address. This decapsulated GRE tunnel behaves like a P2MP (Point-to-multipoint) tunnel, which means that an incoming GRE packet can have any source IP address and matching destination IP address to the tunnel source configured. However, once a source IP address is used for decapsulated P2MP tunnel, it cannot be re-used with other decapsulation tunnels.
- The command `tunnel ttl disable` is supported. This command controls TTL decrement of a packet being encapsulated. After configuring this command for a tunnel interface, TTL value of incoming packet is not decremented by one, and original incoming packet is encapsulated without changing the TTL. By default, `tunnel ttl disable` isn't configured. This means that the TTL of incoming packets is decremented by one before GRE encapsulation.

For example, consider an incoming packet that had the TTL value equal to one. On GRE encapsulation, the TTL value is decremented by one and becomes zero. Therefore the router will discard the packet and send an ICMP message back to the originating host. Using this feature, you can disable TTL decrement and avoid the packet discard.

#### Configuration Example

```
Router#configure
Router(config)#interface tunnel-ip30016
Router(config-if)#tunnel ttl disable
Router(config-if)#commit
```

## Limitations for Configuring GRE Tunnels

This list describes the limitations for configuring GRE tunnels:

- GRE tunnels configured without any decapsulation or encapsulation mode support only ERPSAN feature.
- Don't create multiple GRE/IP-in-IP tunnels with the same pair of source and destination IP address or interface name. Configure all tunnels with unique source-destination pairs. In an encapsulation or decapsulation tunnel where only either source or destination is mentioned, the source-destination pair should also be unique when compared to other encapsulation or decapsulation tunnels.
- Bi-directional GRE tunnel isn't supported.
- Routing protocols over GRE tunnels aren't supported.
- Multicast over GRE isn't supported.
- GRE KA (Keep Alive) isn't supported.
- GRE parameters such as MTU (Maximum Transmission Unit) and key functionalities aren't supported.



## Configure GRE Tunnels

Configuring a GRE tunnel involves creating a tunnel interface and defining the tunnel source and destination. This example shows how to configure a GRE tunnel between source and destination. The router supports only uni-directional GRE with either encapsulation or decapsulation mode.

```
Router# configure
Router(config)# interface tunnel-ip1
Router(config-if)# ipv4 address 101.0.1.2 255.255.255.0
Router(config-if)# ipv6 address 101:0:1::2/64
Router(config-if)# tunnel mode gre ipv4 [encap | decap]
Router(config-if)# tunnel source 2.2.1.1
Router(config-if)# tunnel destination 2.2.2.1/32
Router(config-if)# commit
Router(config-if)# exit
```

To configure ABFv4/v6 over GRE:

```
router static
  address-family ipv4 unicast
    201.0.1.0/24 tunnel-ip1
  address-family ipv6 unicast
    201:0:1::0/64 tunnel-ip1

ipv4 access-list abf-gre
  1 permit ipv4 any any nexthop1 ipv4 201.0.1.2
ipv6 access-list abf6-gre
  1 permit ipv6 any any nexthop1 ipv6 201:0:1::2

interface HundredGigE0/0/0/24
  ipv4 address 24.0.1.1/24
  ipv6 address 24:0:1::1/64
  ipv4 access-group abf-gre ingress
  ipv6 access-group abf6-gre ingress
!
```

To configure MPLS PoP label over GRE:

```
router static
  address-family ipv4 unicast
    201.0.1.0/24 tunnel-ip1
  address-family ipv6 unicast
    201:0:1::0/64 tunnel-ip1

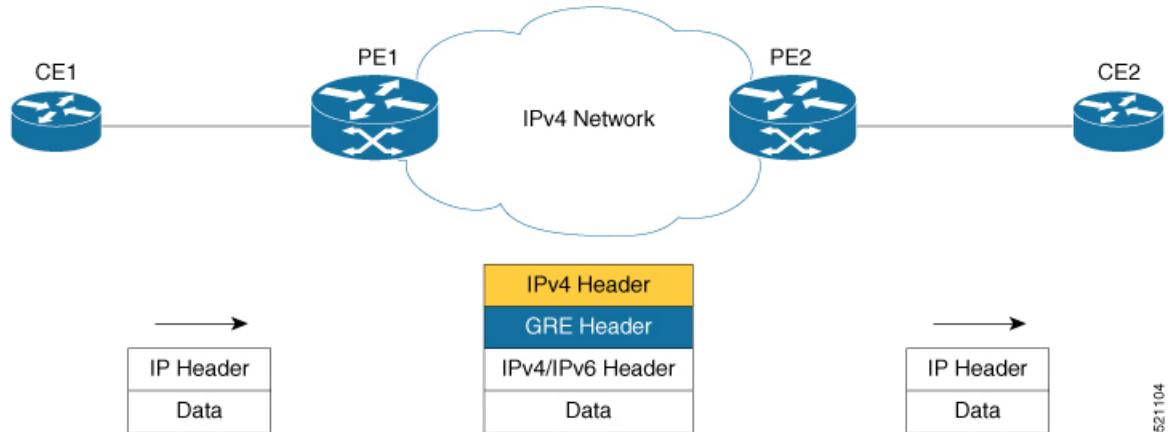
mpls static
  interface HundredGigE0/0/0/24
  lsp gre
    in-label 30501 allocate
    forward path 1 resolve-nexthop 201.0.1.2 out-label pop
!
```



**Note** Bi-directional GRE tunnel supports only ERSPAN.

## Unidirectional GRE Encapsulation (GREv4)

A tunnel configured using encapsulation mode performs encapsulation of IPv4/IPv6 payload inside the GRE header. The following figure shows GRE encapsulation. Routers in the IP cloud have no knowledge of encapsulated IP source address or destination address.



521104

### Configuration

The following example shows how to configure GRE tunnel encapsulation:

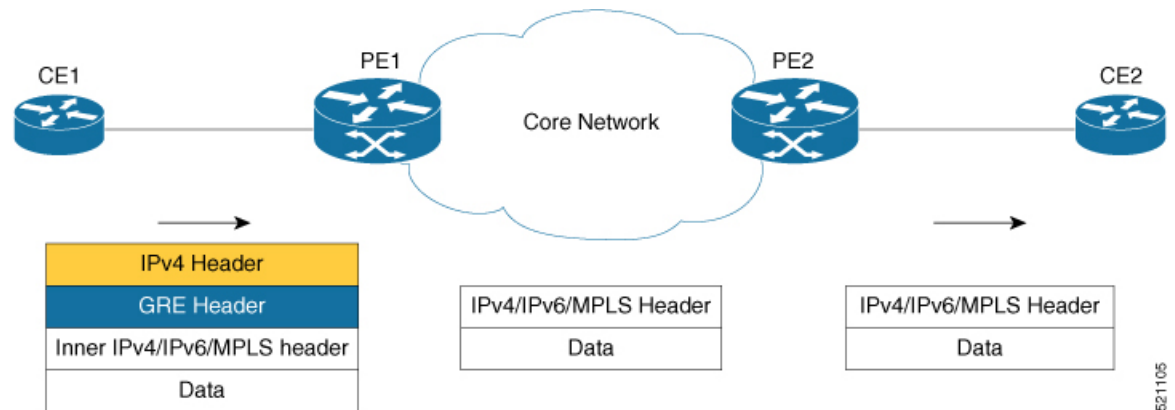
```
interface tunnel-ip1
  ipv4 address 101.0.1.1/24
  ipv6 address 101:0:1::1/64
  tunnel mode gre ipv4 encap
  tunnel source [ loopback1 | <any-ipaddress> | any-interface]
  tunnel destination [ 20.0.1.1/32 | 20.0.1.0/24 | 20.0.1.0/28]

router static
  address-family ipv4 unicast
  201.0.1.0/24 tunnel-1

router static
  address-family ipv6 unicast
  201:0:1::0/64 tunnel-1
```

## Unidirectional GRE Decapsulation (GREv4)

In unidirectional GRE decapsulation, the outer GRE header is decapsulated and the inner IPv4/IPv6/MPLS payload is forwarded to the next hop router. The following figure shows GRE decapsulation. In the figure, PE1 strips off outer GRE header and inner payload is forwarded as regular IPv4/IPv6/MPLS forwarding.



521105

### Configuration

There are two methods to configure GRE tunnel decapsulation:

#### 1. CLI-based tunnel decapsulation configuration

```
interface tunnel-ip1
  ipv4 address 101.0.1.1/24
  ipv6 address 101:0:1::1/64
  tunnel mode gre ipv4 decap
  tunnel source [ loopback1 | <any-ipaddress> | any-interface]
  tunnel destination [ 20.0.1.1/32 | 20.0.1.0/24 | 20.0.1.0/28]
```

#### 2. PBR-based tunnel decapsulation configuration

```
class-map type traffic match-all test_gre1
  match protocol gre
  match destination-address ipv4 10.0.1.2 255.255.255.255
  match source-address ipv4 10.10.10.1 255.255.255.255
end-class-map

policy-map type pbr P1-test
  class type traffic test_gre1 decapsulate gre
vrf-policy vrf default address-family ipv4 policy type pbr input P1-test
```

# ECMP and LAG Hashing for NVGRE Flows

Table 30: Feature History Table

Feature Name	Release Information	Feature Description
ECMP and LAG Hashing for NVGRE Flows	Release 7.5.2	<p>This feature allows transit routers to load balance the GRE traffic, based on GRE payload.</p> <p>A transit node distributes incoming GRE traffic across ECMP and LAG paths in a GRE tunnel topology. A hashing function uses GRE payload that consists of inner Ethernet frame with destination MAC and source MAC addresses, to derive the traffic entropy.</p> <p>ECMP and LAG hashing is enabled on Cisco 8000 series routers by default.</p>

Network Virtualization using Generic Routing Encapsulation (NVGRE) endpoints are network devices that act as interfaces between physical and virtual networks. NVGRE endpoint encapsulates Ethernet data frames to and from GRE tunnel. The encapsulated GRE packet is bridged and routed to the destination. On the destination, the NVGRE endpoint decapsulates the GRE packet to recover the original Ethernet frame. NVGRE is described in RFC 7637.

NVGRE uses the following header information for encapsulation:

Header	Parameters
Outer Ethernet Header	Destination MAC address, Source MAC address
Outer IP Header	IPv4 and IPv6 addresses as delivery protocol
GRE Header	GRE protocol type 0x6558 (transparent Ethernet)
GRE Payload	Inner Ethernet frame with Destination MAC address

For load balancing the GRE traffic, the transit router uses GRE payload that consists of inner Ethernet frame with destination MAC and source MAC addresses. The transit router derives the traffic entropy information from the GRE payload.

The hashing function considers the following parameters of GRE packets, along with Router ID, for load balancing the GRE traffic:

Header	Parameters
Outer IPv4 Header	Source IP address, Destination IP address, IP (GRE)
Outer IPv6 Header	Source IP address, Destination IP address, IP (GRE)

Inner Header	Destination MAC address, Source MAC
--------------	-------------------------------------

**Restrictions for ECMP and LAG Hashing for NVGRE Flows**

ECMP and LAG hashing does not support:

- Outer IPv4 header with Options field.
- Outer IPv6 header with extension headers.





# CHAPTER 11

## Configuring 802.1Q VLAN Interfaces

This module describes the configuration and management of 802.1Q VLAN interfaces.

The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information. It defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure.

The 802.1Q standard is intended to address the problem of how to divide large networks into smaller parts so broadcast and multicast traffic does not use more bandwidth than necessary. The standard also helps provide a higher level of security between segments of internal networks.

### Feature History for Configuring 802.1Q VLAN Interfaces

Release	Modification
Release 7.0.11	This feature was introduced.
Release 7.2.12	Support for Layer 2 interfaces was introduced.

- [Prerequisites for Configuring 802.1Q VLAN Interfaces, on page 201](#)
- [Information About Configuring 802.1Q VLAN Interfaces, on page 202](#)
- [How to Configure 802.1Q VLAN Interfaces, on page 203](#)
- [Configuration Examples for VLAN Interfaces, on page 208](#)

## Prerequisites for Configuring 802.1Q VLAN Interfaces

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before configuring 802.1Q VLAN interfaces, ensure that you meet the following conditions:

- You must have configured a HundredGigE interface, a FourHundredGigE interface, or an Ethernet bundle interface.

# Information About Configuring 802.1Q VLAN Interfaces

To configure 802.1Q VLAN interfaces, you must understand the following concepts:

## 802.1Q VLAN Overview

A VLAN is a group of devices on one or more LANs that you can configure so that the devices can communicate as if they were attached to the same wire. When in fact, they are located on several different LAN segments. Because VLANs are based on logical instead of physical connections, they are flexible for user and host management, bandwidth allocation, and resource optimization.

The IEEE 802.1Q protocol standard addresses the problem of dividing large networks into smaller parts so broadcast and multicast traffic does not consume more bandwidth than necessary. The standard also helps provide a higher level of security between segments of internal networks.

The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames.

Cisco IOS XR software supports VLAN subinterface configuration on 40Gigabit, HundredGig, FourHundredGig, and bundle interfaces.

### 802.1Q Tagged Frames

The IEEE 802.1Q tag-based VLAN uses an extra tag in the MAC header to identify the VLAN membership of a frame across bridges. This tag is used for VLAN and quality of service (QoS) priority identification. The VLANs can be created statically by manual entry or dynamically through Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP). The VLAN ID associates a frame with a specific VLAN and provides the information that switches must process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of Tag Protocol Identifier (TPID) residing within the type and length field of the Ethernet frame and two bytes of Tag Control Information (TCI) which starts after the source address field of the Ethernet frame.

## Subinterfaces

Subinterfaces are logical interfaces that you can create on a hardware interface. These software-defined interfaces allow the segregation of traffic into separate logical channels on a single hardware interface. It also allows for the better utilization of the available bandwidth on the physical interface.

You can distinguish subinterfaces from each other by adding an extension at the end of the interface name and designation. For instance, the system indicates Ethernet subinterface 23 on the physical interface designated TenGigE 0/1/0/0, by TenGigE 0/1/0/0.23.

Before the system allows a subinterface to pass traffic, it must have a valid tagging protocol encapsulation and VLAN identifier assigned. All Ethernet subinterfaces always default to the 802.1Q VLAN encapsulation. However, you must explicitly define the VLAN identifier.

## Subinterface MTU

The system inherits the subinterface maximum transmission unit (MTU) from the physical interface with an additional four bytes allowed for the 802.1Q VLAN tag.



## Native VLAN

The router does not support a native VLAN. However, the equivalent functionality is accomplished using an **encapsulation** command as follows:

```
encapsulation dot1q TAG-ID
```

## Layer 2 VPN on VLANs

The Layer 2 Virtual Private Network (L2VPN) feature enables Service Providers (SPs) to provide Layer 2 services to geographically disparate customer sites.

The configuration model for configuring VLAN attachment circuits (ACs) is similar to the model used for configuring basic VLANs, where the user first creates a VLAN subinterface, and then configures that VLAN in subinterface configuration mode. To create an AC, you need to include the **l2transport** keyword in the **interface** command string to specify that the interface is a Layer 2 interface.

VLAN ACs support three modes of L2VPN operation:

- Basic Dot1Q AC—The AC covers all frames that are received and sent with a specific VLAN tag.
- QinQ AC— Only outer tag (s-tag) of 0x88a8 and inner tag (c-tag) of 0x8100 is supported.

Keep the following in mind when configuring L2VPN on a VLAN:

- Cisco IOS XR software supports 255 ACs per LC.

Use the **show interfaces** command to display AC information.

## How to Configure 802.1Q VLAN Interfaces

This section contains the following procedures:

### Configuring 802.1Q VLAN Subinterfaces

This task explains how to configure 802.1Q VLAN subinterfaces. To remove these subinterfaces, see the “Removing an 802.1Q VLAN Subinterface” section.



---

**Tip** You can programmatically configure and retrieve the VLAN interfaces and subinterfaces parameters using `openconfig-vlan.yang` OpenConfig data model. To get started with using data models, see the *Programmability Configuration Guide for Cisco 8000 Series Routers*.

---

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

```
/* Enter subinterface configuration mode and specifies the interface type, location, and subinterface number. */
```

```
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4.10
```

- Replace the *interface-path-id* argument with one of the following instances:
- Physical Ethernet interface instance, or with an Ethernet bundle instance. Naming notation is *rack/slot/module/port*, and a slash between values is required as part of the notation.
- Ethernet bundle instance. Range is from 1 through 65535.
- Replace the *subinterface* argument with the subinterface value. Range is from 0 through 4095.
- Naming notation is *interface-path-id.subinterface*, and a period between arguments is required as part of the notation.

/\* Set the Layer 2 encapsulation of an interface. \*/

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




---

**Note** • The **dot1q vlan** command is replaced by the **encapsulation dot1q** command on the Cisco 8000 Series Router. It is still available for backward-compatibility, but only for Layer 3 interfaces.

---

/\* Assign an IP address and subnet mask to the subinterface. \*/

```
RP/0/RP0/CPU0:router(config-subif)# ipv4 address 178.18.169.23/24
```

- Replace *ip-address* with the primary IPv4 address for an interface.
- Replace *mask* with the mask for the associated IP subnet. The network mask can be specified in either of two ways:
  - The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means that the corresponding address bit belongs to the network address.
  - The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address.

/\* The **exit** command is not explicitly required. \*/

```
RP/0/RP0/CPU0:router(config-subif)# exit
RP/0/RP0/CPU0:router(config)# end
or
RP/0/RP0/CPU0:router(config)# commit
```

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

### Example

```
RP/0/RP0/CPU0:S3(config)#interface fourHundredGigE 0/5/0/1.100
RP/0/RP0/CPU0:S3(config-subif)#ipv4 address 100.100.100.100/31
RP/0/RP0/CPU0:S3(config-subif)#encapsulation dot1q 100
RP/0/RP0/CPU0:S3(config-subif)#no shutdown
RP/0/RP0/CPU0:S3(config-subif)#commit
Mon Jul  8 23:05:01.979 PDT
RP/0/RP0/CPU0:S3(config-subif)#end
RP/0/RP0/CPU0:S3#show interfaces fourHundredGigE 0/5/0/1.100 brief
Mon Jul  8 23:05:08.784 PDT
```

Intf Name	Intf State	LineP State	Encap Type	MTU (byte)	BW (Kbps)
FH0/5/0/1.100	up	up	802.1Q	1518	400000000

```
RP/0/RP0/CPU0:S3#show interfaces brief location 0/5/CPU0 | include 802.1Q
Mon Jul  8 23:07:43.929 PDT
      FH0/5/0/1.100      up      up      802.1Q  1518  400000000
RP/0/RP0/CPU0:S3#
RP/0/RP0/CPU0:S3#"
```

## Configuring an Attachment Circuit on a VLAN

Use the following procedure to configure an attachment circuit on a VLAN.

### SUMMARY STEPS

1. **configure**
2. **interface [HundredGigE | TenGigE | Bundle-Ether | TenGigE] interface-path id.subinterface l2transport**
3. **encapsulation dot1q vlan-id**
4. **end** or **commit**
5. **show interfaces [HundredGigE | TenGigE] interface-path-id.subinterface**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure</b>  <b>Example:</b> RP/0/RP0/CPU0:router# configure terminal	Enters global configuration mode.
Step 2	<b>interface [HundredGigE   TenGigE   Bundle-Ether   TenGigE] interface-path id.subinterface l2transport</b>  <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface TenGigE 0/1/0/0.1 l2transport	Enters subinterface configuration and specifies the interface type, location, and subinterface number.  • Replace the argument with one of the following instances:

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>Physical Ethernet interface instance, or with an Ethernet bundle instance. Naming notation is <i>rack/slot/module/port</i>, and a slash between values is required as part of the notation.</li> <li>Ethernet bundle instance. Range is from 1 through 65535.</li> <li>Replace the <i>subinterface</i> argument with the subinterface value. Range is from 0 through 4095.</li> <li>Naming notation is <i>instance.subinterface</i>, and a period between arguments is required as part of the notation.</li> <li>You must include the <b>l2transport</b> keyword in the command string; otherwise, the configuration creates a Layer 3 subinterface rather than an AC.</li> </ul>
<b>Step 3</b>	<p><b>encapsulation dot1q</b> <i>vlan-id</i></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 100</pre>	Sets the Layer 2 encapsulation of an interface.
<b>Step 4</b>	<p><b>end</b> or <b>commit</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-if-12)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-if-12)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>When you issue the <b>end</b> command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> <li>- Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>- Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>- Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> </ul> </li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 5</b>	<p><b>show interfaces</b> [<b>HundredGigE</b>   <b>TenGigE</b>] <i>interface-path-id.subinterface</i></p> <p><b>Example:</b></p>	(Optional) Displays statistics for interfaces on the router.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router# show interfaces TenGigE 0/3/0/0.1	

## Removing an 802.1Q VLAN Subinterface

This task explains how to remove 802.1Q VLAN subinterfaces that have been previously configured using the Configuring 802.1Q VLAN subinterfaces section in this module.

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

```
/* Remove the subinterface, which also automatically deletes all the configuration applied to the subinterface.
*/
```

```
RP/0/RP0/CPU0:router(config)# no interface TenGigE 0/2/0/4.10
```

- Replace the *instance* argument with one of the following instances:
  - Physical Ethernet interface instance, or with an Ethernet bundle instance. Naming notation is *rack/slot/module/port*, and a slash between values is required as part of the notation.
  - Ethernet bundle instance. Range is from 1 through 65535.
- Replace the *subinterface* argument with the subinterface value. Range is from 0 through 4095.

Naming notation is *instance.subinterface*, and a period between arguments is required as part of the notation.



**Note** Repeat to remove other VLAN subinterfaces.

```
RP/0/RP0/CPU0:router(config)# end
or
RP/0/RP0/CPU0:router(config)# commit
```

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

# Configuration Examples for VLAN Interfaces

This section contains the following example:

## VLAN Subinterfaces: Example

The following example shows how to create three VLAN subinterfaces at one time:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4.1

RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 100
RP/0/RP0/CPU0:router(config-subif)# ipv4 address 10.0.10.1/24
RP/0/RP0/CPU0:router(config-subif)# interface TenGigE0/2/0/4.2

RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 101
RP/0/RP0/CPU0:router(config-subif)# ipv4 address 10.0.20.1/24
RP/0/RP0/CPU0:router(config-subif)# interface TenGigE0/2/0/4.3

RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 102
RP/0/RP0/CPU0:router(config-subif)# ipv4 address 10.0.30.1/24
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# exit
RP/0/RP0/CPU0:router(config)# exit

RP/0/RP0/CPU0:router# show ethernet trunk bundle-Ether 1
Trunk                               Sub types          Sub states
VLAN trunks: 1,
  1 are 802.1Q (Ether)
Sub-interfaces: 3,
  3 are up.
802.1Q VLANs: 3,
  3 have VLAN Ids,

RP/0/RP0/CPU0:router# show vlan interface

```

Interface	St Ly	MTU	Subs	L3
Te0/2/0/4.1	Up	10	up	
Te0/2/0/4.2	Down	20	up	
Te0/2/0/4.3	Ad-Down	30	up	

```
RP/0/RP0/CPU0:router# show vlan trunks brief

```

Summary	0	1000	1000	0	0	Up L3	1514	1000
Te0/2/0/4			802.1Q (Ether)		up			

The following example shows how to create two VLAN subinterfaces on an Ethernet bundle:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface bundle-ether 2
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.2.1/24
RP/0/RP0/CPU0:router(config-if)# exit
```

```
RP/0/RP0/CPU0:router(config)# interface bundle-ether 2.1

RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 100
RP/0/RP0/CPU0:router(config-subif)# ipv4 address 192.168.100.1/24
RP/0/RP0/CPU0:router(config-subif)# exit
RP/0/RP0/CPU0:router(config)# interface bundle-ether 2.2

RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 200
RP/0/RP0/CPU0:router(config-subif)# ipv4 address 192.168.200.1/24
RP/0/RP0/CPU0:router(config-subif)# exit
RP/0/RP0/CPU0:router(config)# commit
```







# CHAPTER 12

## Configure IP-in-IP Tunnels

This chapter provides conceptual and configuration information for IP-in-IP tunnels.

**Table 31: Feature History for Configure Tunnels**

Release 7.0.11	This feature was introduced.
Release 7.0.14	Support for the following feature was introduced in Configure Tunnels: <ul style="list-style-type: none"> <li>Extended ACL must match on the outer header for IP-in-IP Decapsulation.</li> </ul>

**Table 32: Feature History Table**

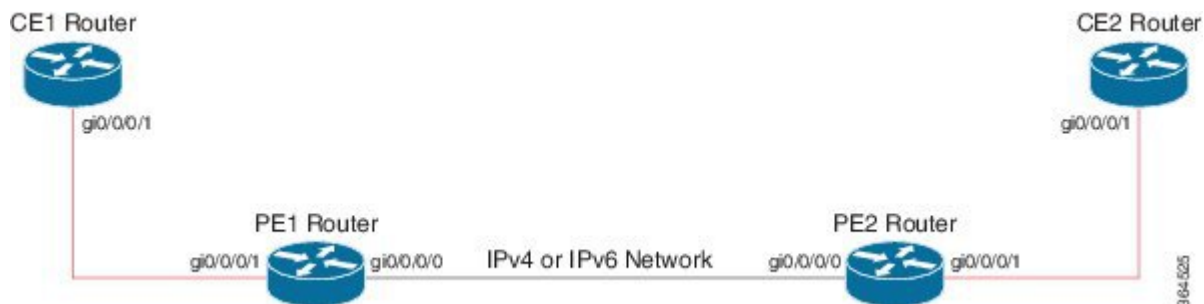
Feature Name	Release Information	Feature Description
IPv4 packets with IPv6 Outer Header	Release 7.5.3	<p>With this release, decapsulation of IPv4 and IPv6 tunnels with IPv6 outer headers are supported. This decapsulation is supported only with <b>tunnel source direct</b> option and not with <b>tunnel source</b> with IPv6 address.</p> <p>This feature helps the administrators to take advantage of the benefits of IPv6, such as improved routing and security, without having to upgrade their entire network to IPv6.</p>

Tunneling provides a mechanism to transport packets of one protocol within another protocol. IP-in-IP tunneling refers to the encapsulation and decapsulation of an IP packet as a payload in another IP packet. Cisco 8000 Series Routers support IP-in-IP decapsulation with all possible combinations of IPv4 and IPv6; that is, IPv4 over IPv4, IPv6 over IPv4, IPv4 over IPv6, and IPv6 over IPv6. For example, an IPv4 over IPv6 refers to an IPv4 packet as a payload encapsulated within an IPv6 packet and routed across an IPv6 network to reach the destination IPv4 network, where it is decapsulated.

IP-in-IP tunneling can be used to connect remote networks securely or provide virtual private network (VPN) services.

The following example provides configurations for an IPv4 or IPv6 tunnel, with the transport VRF as the default VRF for the following simplified network topology.

Figure 12: IP-in-IP Tunnel Network Topology



## Configuration Example for IPv4 Tunnel

PE1 Router Configuration	PE2 Router Configuration
<pre>interface GigabitEthernet0/0/0/0 !! Link between PE1-PE2 ipv4 address 100.1.1.1/64 ! interface GigabitEthernet0/0/0/1 !! Link between CE1-PE1 ipv4 address 20.1.1.1/24 ipv6 address 20::1/64 ! interface tunnel-ip 1 ipv4 address 10.1.1.1/24 ipv6 address 10::1/64 tunnel mode ipv4 tunnel source GigabitEthernet0/0/0/0 tunnel destination 100.1.1.2 !  router static address-family ipv4 unicast  30.1.1.0/24 tunnel-ip1 address-family ipv6 unicast  30::0/64 tunnel-ip1 ! !</pre>	<pre>interface GigabitEthernet0/0/0/0 !! Link between PE1-PE2 ipv4 address 100.1.1.2/64 ! interface GigabitEthernet0/0/0/1 !! Link between PE2-CE2 ipv4 address 30.1.1.1/24 ipv6 address 30::1/64 ! interface tunnel-ip 1 ipv4 address 10.1.1.2/24 ipv6 address 10::2/64 tunnel mode ipv4 tunnel source GigabitEthernet0/0/0/0 tunnel destination 100.1.1.1 !  router static address-family ipv4 unicast  20.1.1.0/24 tunnel-ip1 address-family ipv6 unicast  20::0/64 tunnel-ip1 ! !</pre>
CE1 Router Configuration	CE2 Router Configuration
<pre>interface GigabitEthernet0/0/0/1 !! Link between CE1-PE1 ipv4 address 20.1.1.2 255.255.255.0 ipv6 address 20::2/64 ! router static address-family ipv4 unicast  30.1.1.0/24 20.1.1.1 address-family ipv6 unicast  30::0/64 20::1 ! !</pre>	<pre>interface GigabitEthernet0/0/0/1 !! Link between CE2-PE2 ipv4 address 30.1.1.2 255.255.255.0 ipv6 address 30::2/64 ! router static address-family ipv4 unicast  20.1.1.0/24 30.1.1.1 address-family ipv6 unicast  20::0/64 30::1 ! !</pre>

## Configuration Example for IPv6 Tunnel

PE1 Router Configuration	PE2 Router Configuration
<pre> interface GigabitEthernet0/0/0/0 !! Link between PE1-PE2 ipv6 address 100::1/64 ! interface GigabitEthernet0/0/0/1 !! Link between CE1-PE1 vrf RED ipv4 address 20.1.1.1/24 ipv6 address 20::1/64 ! interface tunnel-ip 1 vrf RED ipv4 address 10.1.1.1/24 ipv6 address 10::1/64 tunnel mode ipv6 tunnel source GigabitEthernet0/0/0/0 tunnel destination 100::2 ! vrf RED address-family ipv6 unicast import route-target 2:1 ! export route-target 2:1 ! address-family ipv4 unicast import route-target 2:1 ! export route-target 2:1 ! router static vrf RED address-family ipv4 unicast 30.1.1.0/24 tunnel-ip1 address-family ipv6 unicast 30::0/64 tunnel-ip1 ! ! ! </pre>	<pre> interface GigabitEthernet0/0/0/0 !! Link between PE1-PE2 ipv6 address 100::2/64 ! interface GigabitEthernet0/0/0/1 !! Link between PE2-CE2 vrf RED ipv4 address 30.1.1.1/24 ipv6 address 30::1/64 ! interface tunnel-ip 1 vrf RED ipv4 address 10.1.1.2/24 ipv6 address 10::2/64 tunnel mode ipv6 tunnel source GigabitEthernet0/0/0/0 tunnel destination 100::1 ! vrf RED address-family ipv6 unicast import route-target 2:1 ! export route-target 2:1 ! address-family ipv4 unicast import route-target 2:1 ! export route-target 2:1 ! router static vrf RED address-family ipv4 unicast 20.1.1.0/24 tunnel-ip1 address-family ipv6 unicast 20::0/64 tunnel-ip1 ! ! ! </pre>
CE1 Router Configuration	CE2 Router Configuration
<pre> interface GigabitEthernet0/0/0/1 !! Link between CE1-PE1 ipv4 address 20.1.1.2 255.255.255.0 ipv6 address 20::2/64 ! router static address-family ipv4 unicast 30.1.1.0/24 20.1.1.1 address-family ipv6 unicast 30::0/64 20::1 ! ! </pre>	<pre> interface GigabitEthernet0/0/0/1 !! Link between CE2-PE2 ipv4 address 30.1.1.2 255.255.255.0 ipv6 address 30::2/64 ! router static address-family ipv4 unicast 20.1.1.0/24 30.1.1.1 address-family ipv6 unicast 20::0/64 30::1 ! ! </pre>

- [IP-in-IP Decapsulation, on page 214](#)

- [ECMP Hashing Support for Load Balancing, on page 222](#)

## IP-in-IP Decapsulation

IP-in-IP encapsulation involves the insertion of an outer IP header over the existing IP header. The source and destination address in the outer IP header point to the endpoints of the IP-in-IP tunnel. The stack of IP headers is used to direct the packet over a predetermined path to the destination, provided the network administrator knows the loopback addresses of the routers transporting the packet. This tunneling mechanism can be used for determining availability and latency for most network architectures. It is to be noted that the entire path from source to the destination does not have to be included in the headers, but a segment of the network can be chosen for directing the packets.

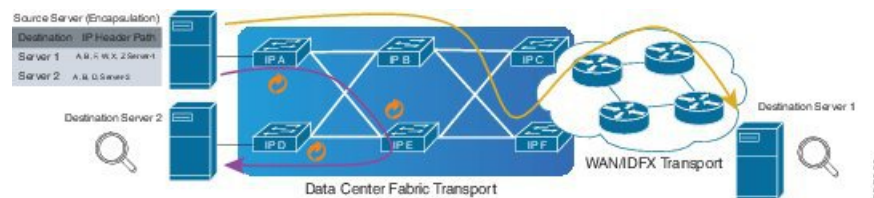
In IP-in-IP encapsulation and decapsulation has two types of packets. The original IP packets that are encapsulated are called Inner packets and the IP header stack added while encapsulation are called the Outer packets.



**Note** The router only supports decapsulation and no encapsulation. Encapsulation is done by remote routers.

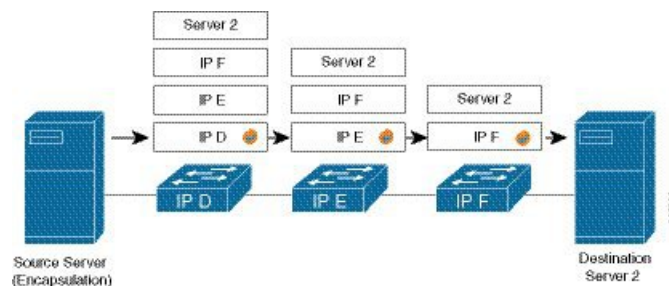
The following topology describes a use case where IP-in-IP encapsulation and decapsulation are used for different segments of the network from source to destination. The IP-in-IP tunnel consists of multiple routers that are used to decapsulate and direct the packet through the data center fabric network.

**Figure 13: IP-in-IP Decapsulation Through a Data Center Network**



The following illustration shows how the stacked IPv4 headers are decapsulated as they traverse through the decapsulating routers.

**Figure 14: IP Header Decapsulation**



### Stacked IP Header in an Encapsulated Packet

The encapsulated packet has an outer IPv4 header that is stacked over the original IPv4 header, as shown in the following illustration.

Figure 15: Encapsulated Packet

[-] Frame	
[-] EthernetII	
Preamble (hex)	fb55555555555d5
Destination MAC	62:19:88:64:E2:68
Source MAC	00:10:94:00:00:02
EtherType (hex)	<auto> Internet IP
[-] IPv4 Header	
Version (int)	<auto> 4
Header length (int)	<auto> 5
ToS/DiffServ	tos (0x00)
Total length (int)	<auto> calculated
Identification (int)	0
[-] Control Flags	
Reserved (bit)	0
DF Bit (bit)	0
MF Bit (bit)	0
Fragment Offset (int)	0
Time to live (int)	255
Protocol (int)	<auto> IP
Checksum (int)	<auto> 33492
Source	192.xx.xx.xx
Destination	127.0.0.1
Header Options	
Gateway	192.0.2.10
[-] IPv4 Header	
Version (int)	<auto> 4
Header length (int)	<auto> 5
ToS/DiffServ	tos (0x00)
Total length (int)	<auto> calculated
Identification (int)	0
[-] Control Flags	
Reserved (bit)	0

385413

### Configuration

You can use the following sample configuration in the routers to decapsulate the packet as it traverses the IP-in-IP tunnel:

```
Router(config)# interface loopback 0
Router(config-if)# ipv4 address 127.0.0.1/32
Router(config-if)# no shutdown
Router(config-if)# interface tunnel-ip 10
```

```
Router(config-if)# ipv4 unnumbered loopback 1
Router(config-if)# tunnel mode ipv4 decap
Router(config-if)# tunnel source loopback 0
```

- **tunnel-ip**: configures an IP-in-IP tunnel interface.
- **ipv4 unnumbered loopback address**: enables ipv4 packet processing without an explicit address, except for loopback address.
- **tunnel mode ipv4 decap**: enables IP-in-IP decapsulation.
- **tunnel source**: indicates the source address for the IP-in-IP decap tunnel with respect to the router interface.




---

**Note** You can configure the tunnel destination only if you want to decapsulate packets from a particular destination. If no tunnel destination is configured, then all the ip-in-ip ingress packets on the configured interface are decapsulated.

---

### Running Configuration

```
Router# show running-config interface tunnel-ip 10
...
interface tunnel-ip 10
ipv4 unnumbered loopback 1
tunnel mode ipv4 decap
```

### Extended ACL to Match the Outer Header for IP-in-IP Decapsulation

Starting with Cisco IOS XR Software Release 7.0.14, extended ACL has to match on the outer header for IP-in-IP Decapsulation. Extended ACL support reduces mirrored traffic throughput. This match is based only on the IPv4 protocol, and extended ACL is applied to the received outermost IP header, even if the outer header is locally terminated.

Sample configuration:

```
Router#show running-config interface bundle-Ether 50.5
Tue May 26 12:11:49.017 UTC
interface Bundle-Ether50.5
ipv4 address 101.1.5.1 255.255.255.0
encapsulation dot1q 5
ipv4 access-group ExtACL_IPinIP ingress
ipv4 access-group any_dscpegg egress
!

Router#show access-lists ipv4 ExtACL_IPinIP hardware ingress location$
Tue May 26 12:11:55.940 UTC
ipv4 access-list ExtACL_IPinIP
10 permit ipv4 192.168.0.0 0.0.255.255 any ttl gt 150
11 deny ipv4 172.16.0.0 0.0.255.255 any fragments
12 permit ipv4 any any
```

## Decapsulation Using Tunnel Source Direct

Table 33: Feature History Table

Feature Name	Release Information	Feature Description
Decapsulating Using Tunnel Source Direct	Release 7.5.3	<p>Tunnel source direct allows you to decapsulate the tunnels on any L3 interface on the router.</p> <p>You can use the <b>tunnel source direct</b> configuration command to choose the specific IP Equal-Cost Multipath (ECMP) links for troubleshooting, when there are multiple IP links between two devices.</p>

To debug faults in various large networks, you may have to capture and analyze the network traffic at a packet level. In datacenter networks, administrators face problems with the volume of traffic and diversity of faults. To troubleshoot faults in a timely manner, DCN administrators must identify affected packets inside large volumes of traffic. They must track them across multiple network components, analyze traffic traces for fault patterns, and test or confirm potential causes.

In some networks, IP-in-IP decapsulation is currently used in network management, to verify ECMP availability and to measure the latency of each path within a datacenter.

The Network Management System (NMS) sends IP-in-IP (IPv4 or IPv6) packets with a stack (multiple) of predefined IPv4 or IPv6 headers (device IP addresses). The destination device at each hop removes the outside header, performs a lookup on the next header, and forwards the packets if a route exists.

Using the **tunnel source direct** command, you can choose the specific IP Equal-Cost Multipath (ECMP) links for troubleshooting, when there are multiple IP links between two devices.



**Tip** You can programmatically configure and manage the Ethernet interfaces using `openconfig-ethernet-if.yang` and `openconfig-interfaces.yang` OpenConfig data models. To get started with using data models, see the *Programmability Configuration Guide for Cisco 8000 Series Routers*.

### Guidelines and Limitations

The following guidelines are applicable to this feature.

- The **tunnel source direct** command is supported only with the tunnel mode as **decap** (when an administrator uses the IP-in-IP decapsulation).
- The source-direct tunnel is always operationally `up` unless it is administratively shut down. The directly connected interfaces are identified using the **show ip route direct** command.
- The **tunnel source direct** command is supported only in IP-in-IP tunneling `decap` mode.
- All Layer 3 interfaces that are configured on the device are supported.

- Platform can accept and program only certain number of IP addresses. The number of IP addresses depends on the make of the platform linecard (LC). Each LC can have different number of Network Processor (NP) slices and interfaces.
- Any inline modification of the **tunnel source direct** command like **tunnel source interface | IP address** is not supported. You must delete the tunnel and recreate it.
- Only one source-direct tunnel per address-family is supported for configuration.
- Regular decapsulation tunnels which have specific source address, are supported. However, the tunnel's specific source address must not be part of any interface.

The following functionalities are not supported for the **tunnel source direct** option.

- GRE tunneling mode.
- VRF (only default VRF is supported).
- ACL and QoS on the tunnels.
- Tunnel encapsulation.
- Tunnel NetIO DLL: Decapsulation is not supported if the packet is punted to slow path.

### Configuration

The **tunnel source direct** configures IP-in-IP tunnel decapsulation on any directly connected IP addresses. This option is now supported only when the IP-in-IP decapsulation is used to source route the packets through the network.

This example shows how to configure IP-in-IP tunnel decapsulation on directly connected IP addresses:

```
Router# configure terminal
Router(config)#interface Tunnel4
Router(config)#tunnel mode ipv4 decap
Router(config)#tunnel source direct
Router(config)#no shutdown
```

This example shows how to configure IP-in-IP tunnel decapsulation on IPv6 enabled networks:

```
Router# configure terminal
Router(config)#interface Tunnel6
Router(config)#tunnel mode ipv6 decap
Router(config)#tunnel source direct
Router(config)#no shutdown
```

### Verifying the Configuration

The following example shows how to verify IP-in-IP tunnel decapsulation with **tunnel source direct** option:

```
Router#show running-config interface tunnel 1
interface Tunnell
  tunnel mode ipv6ipv6 decapsulate-any
  tunnel source direct
  no shutdown

Router#show interface tunnel 1
Tunnell is up    Admin State: up
MTU 1460 bytes, BW 9 Kbit
Tunnel protocol/transport IPv6/DECAPANY/IPv6
```



```
Tunnel source - direct
```

```
Tx 0 packets output, 0 bytes Rx 0 packets input, 0 bytes
```

## Configure Tunnel Destination with an Object Group

Table 34: Feature History Table

Feature Name	Release Information	Description
Configure Tunnel Destination with an Object Group	Release 7.5.4	<p>You can now assign an object group as the destination for an IP-in-IP decapsulation tunnel. With this functionality, you could configure an IPv4 or IPv6 object group consisting of multiple IPv4 or IPv6 addresses as the destination for the tunnel instead of a single IPv4 or IPv6 address. Using an object group instead of a singular IP address. This helps reduce the configuration complexity in the router by replacing the multiple tunnels with one destination with a single decapsulation tunnel that supports a diverse range of destinations</p> <p>The feature introduces these changes:</p> <ul style="list-style-type: none"> <li>• <b>CLI:</b> New <a href="#">tunnel destination</a> command.</li> <li>• <b>YANG Data Model:</b> New <b>object-group</b> option supported in <code>Cisco-IOS-XR-um-iftunnel-cfg.yang</code> Cisco native model (see <a href="#">GitHub</a>).</li> </ul>

In IP-in-IP Decapsulation, the router accepts a packet on a tunneled interface only when the tunnel IP address matches the source IP address of the incoming packets. With this implementation, the user needs to configure separate interface tunnels for each IP address that the router needs to receive the traffic packets. This limitation often leads to configuration overload on the router.

You can eliminate the configuration overload on the router by assigning an object group as the tunnel destination for IPv4 and IPv6 traffic types. That is, the router matches the source IP address of the incoming packet against the object group available as the tunnel destination. The decapsulation tunnel accepts the incoming traffic packets when there's a match between the packet source and the object group. Otherwise, the router drops the packets.

## Restrictions

The following restrictions are applicable to the tunnel destination with an object group feature:

- GRE tunnels don't support configuring object groups as the tunnel destination.
- The router supports configuring tunnel destination with an object group only when the tunnel source is tunnel source direct.
- You can configure the object group as tunnel destination only on default VRF.
- Configuring object groups as the tunnel destination isn't applicable to tunnel encapsulation.
- Subinterfaces don't support configuring object groups as the tunnel destination.
- Configuring object groups as the tunnel destination feature is mutually exclusive with ACL and QoS features.
- The tunnel destination feature supports only IPv4 and IPv6 object groups.
- The router does not support changing tunnel configuration after its creation. Configure the tunnel source direct and tunnel destination with an object group while creating the tunnel only.

## Prerequisites

- Define an object group including the network elements for the tunnel destination.
- Enable the tunnel source direct feature. For more information, see decapsulation using tunnel source direct.

## Configuration Example

This section provides an example for configuring the tunnel destination with an object group:

### Configuration

#### IPv4:

```
Router# configure
/* Configure the IPv4 object group */
Router(config)# object-group network ipv4 Test_IPv4
Router(config-object-group-ipv4)# 192.0.2.0/24
Router(config-object-group-ipv4)# 198.51.100.0/24
Router(config-object-group-ipv4)# 203.0.113.0/24
Router(config-object-group-ipv4)# commit
Router(config-object-group-ipv4)# exit

/* Enters the tunnel configuration mode */
Router(config)# interface tunnel TestIPv4

/* Configures the tunnel mode */
Router(config-if)# tunnel mode ipv4 decap

/* Configures the tunnel to accept all packets with destination address matching the IP
addresses on the router */
Router(config-if)# tunnel source direct

/* Configures the tunnel to accept all packets with destination address that are in the
specified object group */
Router(config-if)# tunnel destination object-group ipv4 Test_IPv4
```

```
Router(config-if) # no shutdown
Router(config-if) # commit
Router(config-if) # exit
```

### IPv6:

```
Router# configure
/* Configure the IPv6 object group */
Router(config)# object-group network ipv6 Test_IPv6
Router(config-object-group-ipv6)# 2001:DB8::/32
Router(config-object-group-ipv6)# 2001:DB8::/48
Router(config-object-group-ipv6)# commit
Router(config-object-group-ipv6)# exit

/* Enters the tunnel configuration mode */
Router(config)# interface tunnel TestIPv6

/* Configures the tunnel mode */
Router(config-if)# tunnel mode ipv6 decap

/* Configures the tunnel to accept all packets with destination address matching the IP
addresses on the router */
Router(config-if)# tunnel source direct

/* Configures the tunnel to accept all packets with destination address that are in the
specified object group */
Router(config-if)# tunnel destination object-group ipv6 Test_IPv6

Router(config-if) # no shutdown
Router(config-if) # commit
Router(config-if) # exit
```

### Running Configuration

```
Router# show running config object-group
object-group network ipv4 Test_IPv4
192.0.2.0/24
198.51.100.0/24
203.0.113.0/24
!
object-group network ipv6 Test_IPv6
2001:DB8::/32
2001:DB8::/48
!

Router# show interface tunnel TestIPv4
interface TunnelTestIPv4
  tunnel mode ipv4 decap
  tunnel source direct
  tunnel destination object-group ipv4 Test_IPv4
  no shutdown
!

Router# show interface tunnel TestIPv6
interface TunnelTestIPv6
  tunnel mode ipv6 decap
  tunnel source direct
  tunnel destination object-group ipv6 Test_IPv6
  no shutdown
!
```

### Verification

```

Router# show tunnel ip ea database

----- node0_0_CPU0 -----
tunnel ifhandle 0x80022cc
tunnel source 161.115.1.2
tunnel destination address group Test_IPv4
tunnel transport vrf table id 0xe0000000
tunnel mode gre ipv4, encap
tunnel bandwidth 100 kbps
tunnel platform id 0x0
tunnel flags 0x40003400
IntfStateUp
BcStateUp
Ipv4Caps
Encap
tunnel mtu 1500
tunnel tos 0
tunnel ttl 255
tunnel adjacency flags 0x1
tunnel o/p interface handle 0x0
tunnel key 0x0, entropy length 0 (mask 0xffffffff)
tunnel QT next 0x0
tunnel platform data (nil)
Platform:
Handle: (nil)
Decap ID: 0
Decap RIF: 0
Decap Recycle Encap ID: 0x00000000
Encap RIF: 0
Encap Recycle Encap ID: 0x00000000
Encap IPv4 Encap ID: 0x4001381b
Encap IPv6 Encap ID: 0x00000000
Encap MPLS Encap ID: 0x00000000
DecFEC DecRcyLIF DecStatsId EncRcyLIF

```

## ECMP Hashing Support for Load Balancing

The system inherently supports the n-tuple hash algorithm. The first inner header in the n-tuple hashing includes the source port and the destination port of UDP / TCP protocol headers.

The load balancing performs these functions:

- Incoming data traffic is distributed over multiple equal-cost connections.
- Incoming data traffic is distributed over multiple equal-cost connections member links within a bundle interface.
- Layer 2 bundle and Layer 3 (network layer) load-balancing decisions are taken on IPv4, and IPv6. If it is an IPv4 or an IPv6 payload, then an n-tuple hashing is done.
- An n-tuple hash algorithm provides more granular load balancing and used for load balancing over multiple equal-cost Layer 3 (network layer) paths. The Layer 3 (network layer) path is on a physical interface or on a bundle interface.
- The n-tuple load-balance hash calculation contains:
  - Source IP address
  - Destination IP address

- IP Protocol type
- Router ID
- Source port
- Destination port
- Input interface
- Flow-label (for IPv6 only)

## User-Defined Fields for ECMP Hashing

Table 35: Feature History Table

Feature Name	Release Information	Description
User-Defined Fields for ECMP Hashing	Release 7.5.5	<p>We ensure that in cases where multiple paths are used to carry packets from source to destination, each path is utilized for this purpose and no path is over-utilized or congested. This is made possible because we now provide customized ECMP hashing fields that are used for path computation.</p> <p>Previously, the router relied on fixed packet header fields for hashing, which were not user configurable. With additional user-defined bytes considered for hashing, the granularity at which the traffic can be analyzed for ECMP load balancing increases, resulting in better load balancing and path utilization.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b></p> <ul style="list-style-type: none"> <li>• <b>cef load-balancing fields user-data</b></li> <li>• The <b>show cef exact-route</b> command is modified with a new <b>user-data</b> keyword.</li> <li>• The <b>show cef ipv4 exact-route</b> command is modified with a new <b>user-data</b> keyword.</li> <li>• The <b>show cef ipv6 exact-route</b> command is modified with a new <b>user-data</b> keyword.</li> </ul> <p><b>YANG:</b></p> <ul style="list-style-type: none"> <li>• New Xpath for <code>Cisco-IOS-XR-8000-fib-platform-cfg.yang</code> (see <a href="#">Github</a>, <a href="#">YANG Data Models Navigator</a>).</li> </ul>

ECMP hashing is used to distribute traffic across multiple equal-cost paths. See [ECMP Hashing Support for Load Balancing, on page 222](#) for the default static hashing algorithm details.

You can now add user-defined packet header fields for ECMP path calculation for ipv4 and ipv6 flows using the **cef load-balancing fields user-data** command. Ensure you specify these user-defined fields based on the type of traffic flow that requires load balancing. You can include the following parameters:

- **Hash header:** The hash header specifies which packet header is being considered for load balancing. You can enable any or all of the available six profiles.
  - IPv4: tcp, udp, non-tcp-udp
  - IPv6: tcp, udp, non-tcp-udp

If any hash header profile is defined for load balancing, along with the fixed fields considered for hashing, additional bytes in the payload are also used for path computation.

- **Hashing offset:** The hashing offset specifies the byte location from the end of the configured header.
- **Hash size:** The hash size specifies the number of bytes that is considered from the start of the hash offset by the ECMP hashing algorithm. Range is 1 to 4 bytes.
- **Location:** This specifies the location of the ingress line card that receives the incoming traffic. The user-defined hashing configuration is applied on the specified line card.

The addition of the user-defined packer header fields increases the granularity at which the traffic is analyzed for ECMP load balancing. When multiple paths with equal cost are available for routing a specific type of packet from a source to a destination, this granularity ensures that the intended type of traffic is evenly distributed across these paths. This ensures all available paths are used efficiently and prevents congestion or over-utilization of a single path.

You can also retrieve the exact-route information based on the configured user-data using the **show cef exact-route** command with **user-data** keyword.



#### Note

- When the user-defined hashing configuration is active, any additional options or optional keywords are disregarded during the parsing of incoming packets for retrieving the user-defined bytes.
- The hashing results based on user-defined hash feature is applicable to BGP/IGP ECMP and LAG hashing.
- The use of the user-defined hashing configuration changes the load balancing behavior of GRE and IPinIP traffic. This includes all traffic that begins with ipv4, ipv6, ipv4+udp, ipv6+udp, ipv4+tcp, and ipv6+tcp, regardless of the payload.

## Configure User-Defined Fields for ECMP Hashing

The command **cef load-balancing fields user-data** configures the additional user-defined fields that are to be considered for the hashing algorithm.

This example shows how to configure the additional IPv4 header fields for TCP packets:

```
Router# configure terminal
Router(config)# cef load-balancing fields user-data ipv4 tcp offset 5 size 3 location 0/0/CPU0
Router(config)# commit
```

- offset 5: The payload considered for hashing starts from byte 6 from the end of TCP header.
- size 3: Three bytes of payload are considered.
- location 0/0/CPU0: Specifies the line card on which the configuration is applied.

In the above example, the sixth, seventh, and eighth bytes of the payload are considered additionally for the hashing.

This example shows how to configure the additional IPv6 header fields for UDP packets:

```
Router# configure terminal
Router(config)# cef load-balancing fields user-data ipv6 udp offset 0 size 2 location 0/0/CPU0
Router(config)# commit
```

- offset 0: The payload considered for hashing starts from the end of UDP header.
- size 2: Two bytes of payload are considered.
- location 0/0/CPU0: Specifies the line card on which the configuration is applied.

In the above example, the first two bytes of payload of a UDP packet are considered additionally for the hashing.

## Running Configuration

The following example shows the running configuration:

```
Router# show running-config | include cef
Fri Jul 28 12:02:01.002 UTC
cef load-balancing fields user-data ipv4 tcp offset 5 size 3 location 0/0/CPU0
cef load-balancing fields user-data ipv6 udp offset 0 size 2 location 0/0/CPU0
Router#
```

## Verification

The following example shows the difference in load balancing before and after applying user-defined hashing, for a flow with data that exhibits good hashing behavior.

### Before applying user-defined hashing

```
Router# show interfaces accounting | i IPV6_U
Protocol          Pkts In      Chars In      Pkts Out      Chars Out
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      2            144            0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      0              0            3979416        1981749168
IPV6_UNICAST      4191438       2087336124    0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
Router#
```

### After applying user-defined hashing

```
Router# show interfaces accounting | i IPV6_U
Protocol          Pkts In      Chars In      Pkts Out      Chars Out
IPV6_UNICAST      0              0              39119          19481262
IPV6_UNICAST      0              0              39801          19820898
IPV6_UNICAST      0              0              40483          20160534
```



IPV6_UNICAST	0	0	40524	20180952
IPV6_UNICAST	0	0	40573	20205354
IPV6_UNICAST	0	0	40614	20225772
IPV6_UNICAST	0	0	39368	19605264
IPV6_UNICAST	0	0	40734	20285532
IPV6_UNICAST	0	0	40777	20306946
IPV6_UNICAST	0	0	40171	20005158
IPV6_UNICAST	0	0	40858	20347284
IPV6_UNICAST	0	0	40269	20053962
IPV6_UNICAST	0	0	41603	20718294
IPV6_UNICAST	0	0	40363	20100774
IPV6_UNICAST	0	0	40407	20122686
IPV6_UNICAST	0	0	41098	20466804
IPV6_UNICAST	850393	423495714	0	0

To view the exact route information allocated to the packets, use **show cef exact-route** command with **user-data** keyword.

The packet contains value 0x2 in the packet position for the ipv6 packet, for which the user-defined configuration has been added for a non-tcp-udp ipv6 flow.

```
Router#show cef ipv6 exact-route 100::10 60::1 flow-label 0 protocol 59 source-port 0
destination-port 0 user-data 0x2 ingress-interface HundredGigE0/0/0/2 location 0/0/cpu0
Unsupported protocol value 59
60::/16, version 1293, internal 0x1000001 0x20 (ptr 0x8b78ef00) [1], 0x400 (0x8e9cfc48),
0x0 (0x0)
Updated Aug 14 07:50:20.022
local adjacency to Bundle-Ether3.30

Prefix Len 16, traffic index 0, precedence n/a, priority 2
via Bundle-Ether3.30
via fe80::72b3:17ff:feae:d703/128, Bundle-Ether3.30, 7 dependencies, weight 0, class 0
[flags 0x0]
path-idx 7 NHID 0x0 [0x8db8bed8 0x0]
next hop fe80::72b3:17ff:feae:d703/128
local adjacency
```





# CHAPTER 13

## Configuring Generic UDP Encapsulation

Read this section to get an overview and know how to configure the Generic UDP Encapsulation.

**Table 36: Feature History Table**

Feature Name	Release Information	Feature Description
Generic UDP Encapsulation	Release 7.3.1	<p>This feature enables you to add an additional header to packets to identify or authenticate the data using UDP. Encapsulating packets in UDP leverages the use of the UDP source port to provide entropy to Equal Cost Multi-Path (ECMP) hashing. It provides significant performance benefits for load-balancing.</p> <p>This command is introduced for this feature:</p> <p><b>decapsulate gue</b></p>

- [Understand Generic UDP Encapsulation, on page 229](#)

## Understand Generic UDP Encapsulation

UDP encapsulation is a technique of adding network headers to packets and then encapsulating the packets within the User Datagram Protocol (UDP).

Encapsulating packets using UDP facilitates efficient transport across networks. By leveraging Receive Side Scaling (RSS) and Equal Cost Multipath (ECMP) routing, UDP provides significant performance benefits for load-balancing. The use of the UDP source port provides entropy to ECMP hashing and provides the ability to use the IP source or destination, and the L4 Port for load-balancing entropy.

Traditional mechanisms like Generic Routing Encapsulation (GRE) can handle only the outer Source IP address and parts of the destination address. They may not provide sufficient load balancing entropy.

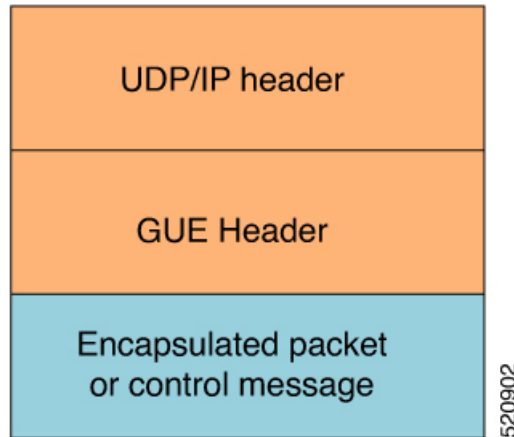
Generic UDP Encapsulation (GUE) is a UDP-based network encapsulation protocol that encapsulates IPv4 and IPv6 packets. GUE provides native UDP encapsulation and defines an additional header, which helps to

determine the payload carried by the IP packet. The additional header can include items, such as a virtual networking identifier, security data for validating or authenticating the GUE header, congestion control data, and so on.

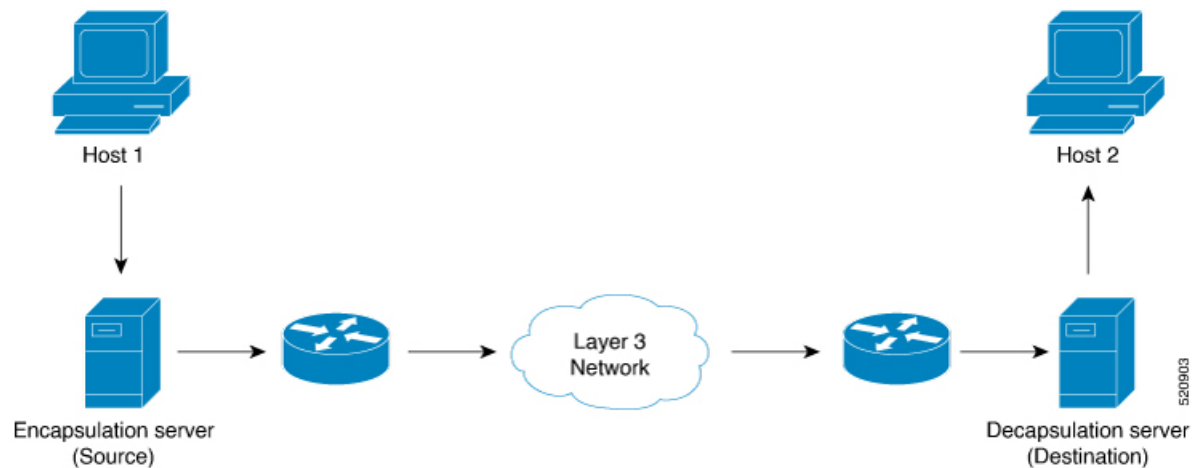
In GUE, the payload is encapsulated in an IP packet that can be IPv4 or IPv6 Carrier. The UDP header is added to provide extra hashing parameters, and optional payload demultiplexing. At the decapsulation node, the Carrier IP and UDP headers are removed, and the packet is forwarded based on the inner payload.

A GUE packet has the general format:

**Figure 16: GUE Packet Format**



For example, in this scenario, if the data stream is sent from Host 1 to Host 2. The server acts as a GUE encapsulator that sends the packets from Host 1. The server, on the other end receiving the data, validates the data for the valid carrier IP and UDP header and decapsulates the data.



GUE has various variants, but variant 1 of GUE allows direct encapsulation of IPv4 and IPv6 in UDP. This technique saves encapsulation overhead on links for the use of IP encapsulation, and also need not allocate a separate UDP port number for IP-over-UDP encapsulation.

Variant 1 has no GUE header, but a UDP packet carries an IP packet. The first two bits of the UDP payload is the GUE variant field and match with the first two bits of the version number in the IP header.

### Benefits of using GUE

- Allows direct encapsulation of payloads, such as IPv4 and IPv6 in the UDP packet.
  - You can use UDP port for demultiplexing payloads.
  - You can use a single UDP port, allowing systems to employ parsing models to identify payloads.
- Leverages the UDP header for entropy labels by encoding a tuple-based source port.
- Leverages source IP addresses for load-balance encoding. The destination too could be terminated based on a subnet providing additional bits for entropy.
- Avoids special handling for transit nodes because they only see an IP-UDP packet with some payload..
- Eases implementation of UDP tunneling with GUE. This is because of the direct encapsulation method of the payloads into UDP.

## Restrictions

- Supports Generic UDP Decapsulation for only variant 1.
- Receives IPv4 packets with the defined GUE port of 6080.
- Decapsulates IPv6 packets with the defined GUE port of 6615.
- Receives MPLS packets with the UDPO MPLS port of 6635.
- Range of source or destination ports is not supported.
- Range, Source, or Destination addresses are not supported, but subnet mask entries are allowed.
- To perform decapsulation, a destination Port is mandatory.
- Terminating GRE after GUE or GUE after GRE is not supported.
- Terminating a label such as a VPN Deaggregation after GUE termination is not supported.
- Slow path support is not supported. To resolve the inner IP Adjacency, use the **cef proactive-arp-nd enable** command.
- Running the **clear all** command doesn't clear the interface of all its existing configurations.

## Configure GUE

### Configuring GUE

Use the following configuration workflow to configure GUE:

1. Configure separate GUE decap tunnel UDP destination port numbers for IPv4, IPv6, and MPLS using **hw-module profile gue udp-dest-port** command.
2. Configure a traffic class: Create a traffic class and specify various criteria for classifying packets using the match commands, and an instruction on how to evaluate these match commands.
3. Configure a policy map: Define a policy map and associate the traffic class with the traffic policy.

4. Apply the policy for each VRF, and apply this policy on all the interfaces that are part of the VRF.

### Configuration Example for GUE IPv4

1. Configure separate UDP port numbers for IPv4, IPv6, and MPLS using **hw-module profile gue udp-dest-port** command.

```
Router# configure
Router# hw-module profile gue udp-dest-port ipv4 6080 ipv6 6080 mpls 6635
Router# commit
```



**Note** While adding or removing the **hw-module profile gue udp-dest-port** command, you must reload the router.

2. Configure a traffic class:

```
Router# configure
Router(config)# class-map type traffic match-all udp-v4
Router(config-cmap)# match destination-address ipv4 220.100.20.0 255.255.255.255
Router(config-cmap)# match source-address ipv4 210.100.20.0 255.255.255.255
Router(config-cmap)# match protocol udp
Router(config-cmap)# match destination-port 6080
Router(config-cmap)# end-class-map
Router(config)# commit
```

```
Router(config)# class-map type traffic match-all udp-mpls1
Router(config-cmap)# match destination-address ipv4 220.100.20.0 255.255.255.255
Router(config-cmap)# match source-address ipv4 210.100.20.0 255.255.255.255
Router(config-cmap)# match protocol udp
Router(config-cmap)# match destination-port 6635
Router(config-cmap)# end-class-map
Router(config)# commit
```

```
Router(config)# class-map type traffic match-all udp-v6
Router(config-cmap)# match destination-address ipv4 220.100.20.0 255.255.255.255
Router(config-cmap)# match source-address ipv4 210.100.20.0 255.255.255.255
Router(config-cmap)# match protocol udp
Router(config-cmap)# match destination-port 6080
Router(config-cmap)# end-class-map
Router(config)# commit
```

3. Define a policy map, and associate the traffic class with the traffic policy:

```
Router(config)# policy-map type pbr magic-decap

Router(config-pmap)# class type traffic udp-v4
Router(config-pmap-c)# decapsulate gue variant 1
Router(config-pmap-c)# exit

Router(config-pmap)# class type traffic udp-v6
Router(config-pmap-c)# decapsulate gue variant 1
Router(config-pmap-c)# exit

Router(config-pmap)# class type traffic udp-mpls1
Router(config-pmap-c)# decapsulate gue variant 1
Router(config-pmap-c)# exit
```

```

Router(config-pmap)# class type traffic class-default
Router(config-pmap-c)# exit
Router(config-pmap)# end-policy-map
Router(config)# commit
Router(config)# exit

```

#### 4. Apply the policy for each VRF:

```

Router# configure
Router(config)# vrf-policy
Router(config-vrf-policy)# vrf default address-family ipv4 policy type pbr input magic-decap
Router(config-vrf-policy)# commit

```

#### Running Configuration:

```

class-map type traffic match-all udp-v4
  match destination-address ipv4 220.100.20.0 255.255.255.255
  match source-address ipv4 210.100.20.0 255.255.255.255
  match protocol udp
  match destination-port 6080
end-class-map
!
class-map type traffic match-all udp-v6
  match destination-address ipv4 220.100.20.0 255.255.255.255
  match source-address ipv4 210.100.20.0 255.255.255.255
  match protocol udp
  match destination-port 6080
end-class-map
!
class-map type traffic match-all udp-mpls1
  match destination-address ipv4 220.100.20.0 255.255.255.255
  match source-address ipv4 210.100.20.0 255.255.255.255
  match protocol udp
  match destination-port 6635
end-class-map
!
policy-map type pbr magic-decap
  class type traffic udp-v4
    decapsulate gue variant 1
  !
  class type traffic udp-v6
    decapsulate gue variant 1
  !
  class type traffic udp-mpls1
    decapsulate gue variant 1
  !
  class type traffic class-default
  !
end-policy-map
!

vrf-policy
  vrf default address-family ipv4 policy type pbr input magic-decap
!

```

#### Verification

To view the set of counter values accumulated for the packets that match the class-map:

```

Router# show policy-map type pbr addr-family ipv4 statistics

VRF Name:      default
Policy-Name:   pmap
Policy Type:   pbr

```

```

Addr Family:   IPv4

Class:   cmap-loop1
  Classification statistics      (packets/bytes)
    Matched      :                0/0
  Transmitted statistics      (packets/bytes)
    Total Transmitted :                0/0

Class:   cmap-loop6
  Classification statistics      (packets/bytes)
    Matched      :                0/0
  Transmitted statistics      (packets/bytes)
    Total Transmitted :                0/0

Class:   cmap-loop2
  Classification statistics      (packets/bytes)
    Matched      :                0/0
  Transmitted statistics      (packets/bytes)
    Total Transmitted :                0/0

Class:   cmap-loop3
  Classification statistics      (packets/bytes)
    Matched      :      198325306/17849277540
  Transmitted statistics      (packets/bytes)
    Total Transmitted :      198325306/17849277540

Class:   cmap-loop4
  Classification statistics      (packets/bytes)
    Matched      :                0/0
  Transmitted statistics      (packets/bytes)
    Total Transmitted :                0/0

```

To clear the policy-map counters for each class-map rule, use the **clear vrf** command:

```
Router# clear vrf default address-family ipv4 statistics
```





## CHAPTER 14

# Controlling the TTL Value of Inner Payload Header

Cisco 8000 Routers allow you to control the TTL value of inner payload header of IP-in-IP tunnel packets before it gets forwarded to the next-hop router. This feature enables a router to forward custom formed IP-in-IP stacked packets even if the inner packet TTL is 1. Therefore, this feature enables you to measure the link-state and path reachability from end to end in a network.



**Note** After you enable or disable the decrement of the TTL value of the inner payload header of a packet, you do not need to reload the line card.

### Configuration

To disable the decrement of the TTL value of inner payload header of an IP-in-IP packet, use the following steps:

1. Enter the global configuration mode.
2. Disable the decrement of TTL value of inner payload header of an IP-in-IP packet.

### Configuration Example

```
/* Enter the Global Configuration mode. */
Router# configure

/* Disable the decrement of TTL value of inner payload header of an IP-in-IP packet. */
Router(config)# hw-module profile cef ttl tunnel-ip decrement disable
Router(config)# commit
```

### Associated Commands

- [hw-module profile cef ttl tunnel-ip decrement disable](#)
- [IP-in-IP Decapsulation, on page 236](#)
- [ECMP Hashing Support for Load Balancing, on page 244](#)

## IP-in-IP Decapsulation

IP-in-IP encapsulation involves the insertion of an outer IP header over the existing IP header. The source and destination address in the outer IP header point to the endpoints of the IP-in-IP tunnel. The stack of IP headers is used to direct the packet over a predetermined path to the destination, provided the network administrator knows the loopback addresses of the routers transporting the packet. This tunneling mechanism can be used for determining availability and latency for most network architectures. It is to be noted that the entire path from source to the destination does not have to be included in the headers, but a segment of the network can be chosen for directing the packets.

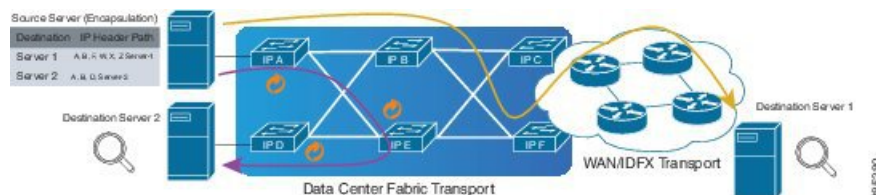
In IP-in-IP encapsulation and decapsulation has two types of packets. The original IP packets that are encapsulated are called Inner packets and the IP header stack added while encapsulation are called the Outer packets.



**Note** The router only supports decapsulation and no encapsulation. Encapsulation is done by remote routers.

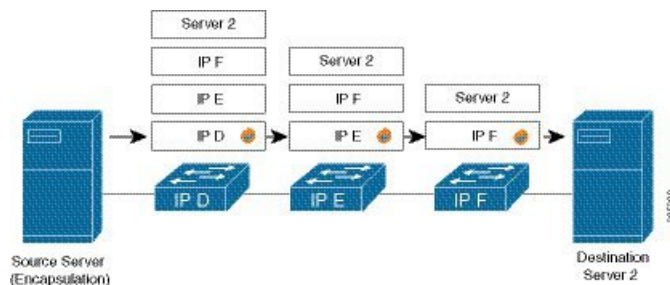
The following topology describes a use case where IP-in-IP encapsulation and decapsulation are used for different segments of the network from source to destination. The IP-in-IP tunnel consists of multiple routers that are used to decapsulate and direct the packet through the data center fabric network.

**Figure 17: IP-in-IP Decapsulation Through a Data Center Network**



The following illustration shows how the stacked IPv4 headers are decapsulated as they traverse through the decapsulating routers.

**Figure 18: IP Header Decapsulation**



### Stacked IP Header in an Encapsulated Packet

The encapsulated packet has an outer IPv4 header that is stacked over the original IPv4 header, as shown in the following illustration.

Figure 19: Encapsulated Packet

[-] Frame	
[-] <b>EthernetII</b>	
Preamble (hex)	fb555555555555d5
Destination MAC	62:19:88:64:E2:68
Source MAC	00:10:94:00:00:02
EtherType (hex)	<auto> Internet IP
[-] <b>IPv4 Header</b>	
Version (int)	<auto> 4
Header length (int)	<auto> 5
ToS/DiffServ	tos (0x00)
Total length (int)	<auto> calculated
Identification (int)	0
[-] <b>Control Flags</b>	
Reserved (bit)	0
DF Bit (bit)	0
MF Bit (bit)	0
Fragment Offset (int)	0
Time to live (int)	255
Protocol (int)	<auto> IP
Checksum (int)	<auto> 33492
Source	192.xx.xx.xx
Destination	127.0.0.1
Header Options	
Gateway	192.0.2.10
[-] <b>IPv4 Header</b>	
Version (int)	<auto> 4
Header length (int)	<auto> 5
ToS/DiffServ	tos (0x00)
Total length (int)	<auto> calculated
Identification (int)	0
[-] <b>Control Flags</b>	
Reserved (bit)	0

385413

### Configuration

You can use the following sample configuration in the routers to decapsulate the packet as it traverses the IP-in-IP tunnel:

```
Router(config)# interface loopback 0
Router(config-if)# ipv4 address 127.0.0.1/32
Router(config-if)# no shutdown
Router(config-if)# interface tunnel-ip 10
```

```
Router(config-if)# ipv4 unnumbered loopback 1
Router(config-if)# tunnel mode ipv4 decap
Router(config-if)# tunnel source loopback 0
```

- **tunnel-ip**: configures an IP-in-IP tunnel interface.
- **ipv4 unnumbered loopback address**: enables ipv4 packet processing without an explicit address, except for loopback address.
- **tunnel mode ipv4 decap**: enables IP-in-IP decapsulation.
- **tunnel source**: indicates the source address for the IP-in-IP decap tunnel with respect to the router interface.




---

**Note** You can configure the tunnel destination only if you want to decapsulate packets from a particular destination. If no tunnel destination is configured, then all the ip-in-ip ingress packets on the configured interface are decapsulated.

---

### Running Configuration

```
Router# show running-config interface tunnel-ip 10
...
interface tunnel-ip 10
ipv4 unnumbered loopback 1
tunnel mode ipv4 decap
```

### Extended ACL to Match the Outer Header for IP-in-IP Decapsulation

Starting with Cisco IOS XR Software Release 7.0.14, extended ACL has to match on the outer header for IP-in-IP Decapsulation. Extended ACL support reduces mirrored traffic throughput. This match is based only on the IPv4 protocol, and extended ACL is applied to the received outermost IP header, even if the outer header is locally terminated.

Sample configuration:

```
Router#show running-config interface bundle-Ether 50.5
Tue May 26 12:11:49.017 UTC
interface Bundle-Ether50.5
ipv4 address 101.1.5.1 255.255.255.0
encapsulation dot1q 5
ipv4 access-group ExtACL_IPinIP ingress
ipv4 access-group any_dscpegg egress
!

Router#show access-lists ipv4 ExtACL_IPinIP hardware ingress location$
Tue May 26 12:11:55.940 UTC
ipv4 access-list ExtACL_IPinIP
10 permit ipv4 192.168.0.0 0.0.255.255 any ttl gt 150
11 deny ipv4 172.16.0.0 0.0.255.255 any fragments
12 permit ipv4 any any
```

## Decapsulation Using Tunnel Source Direct

Table 37: Feature History Table

Feature Name	Release Information	Feature Description
Decapsulating Using Tunnel Source Direct	Release 7.5.3	<p>Tunnel source direct allows you to decapsulate the tunnels on any L3 interface on the router.</p> <p>You can use the <b>tunnel source direct</b> configuration command to choose the specific IP Equal-Cost Multipath (ECMP) links for troubleshooting, when there are multiple IP links between two devices.</p>

To debug faults in various large networks, you may have to capture and analyze the network traffic at a packet level. In datacenter networks, administrators face problems with the volume of traffic and diversity of faults. To troubleshoot faults in a timely manner, DCN administrators must identify affected packets inside large volumes of traffic. They must track them across multiple network components, analyze traffic traces for fault patterns, and test or confirm potential causes.

In some networks, IP-in-IP decapsulation is currently used in network management, to verify ECMP availability and to measure the latency of each path within a datacenter.

The Network Management System (NMS) sends IP-in-IP (IPv4 or IPv6) packets with a stack (multiple) of predefined IPv4 or IPv6 headers (device IP addresses). The destination device at each hop removes the outside header, performs a lookup on the next header, and forwards the packets if a route exists.

Using the **tunnel source direct** command, you can choose the specific IP Equal-Cost Multipath (ECMP) links for troubleshooting, when there are multiple IP links between two devices.



**Tip** You can programmatically configure and manage the Ethernet interfaces using `openconfig-ethernet-if.yang` and `openconfig-interfaces.yang` OpenConfig data models. To get started with using data models, see the *Programmability Configuration Guide for Cisco 8000 Series Routers*.

### Guidelines and Limitations

The following guidelines are applicable to this feature.

- The **tunnel source direct** command is supported only with the tunnel mode as **decap** (when an administrator uses the IP-in-IP decapsulation).
- The source-direct tunnel is always operationally `up` unless it is administratively shut down. The directly connected interfaces are identified using the **show ip route direct** command.
- The **tunnel source direct** command is supported only in IP-in-IP tunneling `decap` mode.
- All Layer 3 interfaces that are configured on the device are supported.

- Platform can accept and program only certain number of IP addresses. The number of IP addresses depends on the make of the platform linecard (LC). Each LC can have different number of Network Processor (NP) slices and interfaces.
- Any inline modification of the **tunnel source direct** command like **tunnel source interface | IP address** is not supported. You must delete the tunnel and recreate it.
- Only one source-direct tunnel per address-family is supported for configuration.
- Regular decapsulation tunnels which have specific source address, are supported. However, the tunnel's specific source address must not be part of any interface.

The following functionalities are not supported for the **tunnel source direct** option.

- GRE tunneling mode.
- VRF (only default VRF is supported).
- ACL and QoS on the tunnels.
- Tunnel encapsulation.
- Tunnel NetIO DLL: Decapsulation is not supported if the packet is punted to slow path.

### Configuration

The **tunnel source direct** configures IP-in-IP tunnel decapsulation on any directly connected IP addresses. This option is now supported only when the IP-in-IP decapsulation is used to source route the packets through the network.

This example shows how to configure IP-in-IP tunnel decapsulation on directly connected IP addresses:

```
Router# configure terminal
Router(config)#interface Tunnel4
  Router(config)#tunnel mode ipv4 decap
  Router(config)#tunnel source direct
  Router(config)#no shutdown
```

This example shows how to configure IP-in-IP tunnel decapsulation on IPv6 enabled networks:

```
Router# configure terminal
Router(config)#interface Tunnel6
  Router(config)#tunnel mode ipv6 decap
  Router(config)#tunnel source direct
  Router(config)#no shutdown
```

### Verifying the Configuration

The following example shows how to verify IP-in-IP tunnel decapsulation with **tunnel source direct** option:

```
Router#show running-config interface tunnel 1
interface Tunnell
  tunnel mode ipv6ipv6 decapsulate-any
  tunnel source direct
  no shutdown

Router#show interface tunnel 1
Tunnell is up    Admin State: up
MTU 1460 bytes, BW 9 Kbit
Tunnel protocol/transport IPv6/DECAPANY/IPv6
```

```
Tunnel source - direct
```

```
Tx 0 packets output, 0 bytes Rx 0 packets input, 0 bytes
```

## Configure Tunnel Destination with an Object Group

Table 38: Feature History Table

Feature Name	Release Information	Description
Configure Tunnel Destination with an Object Group	Release 7.5.4	<p>You can now assign an object group as the destination for an IP-in-IP decapsulation tunnel. With this functionality, you could configure an IPv4 or IPv6 object group consisting of multiple IPv4 or IPv6 addresses as the destination for the tunnel instead of a single IPv4 or IPv6 address. Using an object group instead of a singular IP address. This helps reduce the configuration complexity in the router by replacing the multiple tunnels with one destination with a single decapsulation tunnel that supports a diverse range of destinations</p> <p>The feature introduces these changes:</p> <ul style="list-style-type: none"> <li>• <b>CLI:</b> New <a href="#">tunnel destination</a> command.</li> <li>• <b>YANG Data Model:</b> New <b>object-group</b> option supported in <code>Cisco-IOS-XR-um-iftunnel-cfg.yang</code> Cisco native model (see <a href="#">GitHub</a>).</li> </ul>

In IP-in-IP Decapsulation, the router accepts a packet on a tunneled interface only when the tunnel IP address matches the source IP address of the incoming packets. With this implementation, the user needs to configure separate interface tunnels for each IP address that the router needs to receive the traffic packets. This limitation often leads to configuration overload on the router.

You can eliminate the configuration overload on the router by assigning an object group as the tunnel destination for IPv4 and IPv6 traffic types. That is, the router matches the source IP address of the incoming packet against the object group available as the tunnel destination. The decapsulation tunnel accepts the incoming traffic packets when there's a match between the packet source and the object group. Otherwise, the router drops the packets.

## Restrictions

The following restrictions are applicable to the tunnel destination with an object group feature:

- GRE tunnels don't support configuring object groups as the tunnel destination.
- The router supports configuring tunnel destination with an object group only when the tunnel source is tunnel source direct.
- You can configure the object group as tunnel destination only on default VRF.
- Configuring object groups as the tunnel destination isn't applicable to tunnel encapsulation.
- Subinterfaces don't support configuring object groups as the tunnel destination.
- Configuring object groups as the tunnel destination feature is mutually exclusive with ACL and QoS features.
- The tunnel destination feature supports only IPv4 and IPv6 object groups.
- The router does not support changing tunnel configuration after its creation. Configure the tunnel source direct and tunnel destination with an object group while creating the tunnel only.

## Prerequisites

- Define an object group including the network elements for the tunnel destination.
- Enable the tunnel source direct feature. For more information, see decapsulation using tunnel source direct.

## Configuration Example

This section provides an example for configuring the tunnel destination with an object group:

### Configuration

#### IPv4:

```
Router# configure
/* Configure the IPv4 object group */
Router(config)# object-group network ipv4 Test_IPv4
Router(config-object-group-ipv4)# 192.0.2.0/24
Router(config-object-group-ipv4)# 198.51.100.0/24
Router(config-object-group-ipv4)# 203.0.113.0/24
Router(config-object-group-ipv4)# commit
Router(config-object-group-ipv4)# exit

/* Enters the tunnel configuration mode */
Router(config)# interface tunnel TestIPv4

/* Configures the tunnel mode */
Router(config-if)# tunnel mode ipv4 decap

/* Configures the tunnel to accept all packets with destination address matching the IP
addresses on the router */
Router(config-if)# tunnel source direct

/* Configures the tunnel to accept all packets with destination address that are in the
specified object group */
Router(config-if)# tunnel destination object-group ipv4 Test_IPv4
```



```
Router(config-if) # no shutdown
Router(config-if) # commit
Router(config-if) # exit
```

### IPv6:

```
Router# configure
/* Configure the IPv6 object group */
Router(config)# object-group network ipv6 Test_IPv6
Router(config-object-group-ipv6)# 2001:DB8::/32
Router(config-object-group-ipv6)# 2001:DB8::/48
Router(config-object-group-ipv6)# commit
Router(config-object-group-ipv6)# exit

/* Enters the tunnel configuration mode */
Router(config)# interface tunnel TestIPv6

/* Configures the tunnel mode */
Router(config-if)# tunnel mode ipv6 decap

/* Configures the tunnel to accept all packets with destination address matching the IP
addresses on the router */
Router(config-if)# tunnel source direct

/* Configures the tunnel to accept all packets with destination address that are in the
specified object group */
Router(config-if)# tunnel destination object-group ipv6 Test_IPv6

Router(config-if) # no shutdown
Router(config-if) # commit
Router(config-if) # exit
```

### Running Configuration

```
Router# show running config object-group
object-group network ipv4 Test_IPv4
192.0.2.0/24
198.51.100.0/24
203.0.113.0/24
!
object-group network ipv6 Test_IPv6
2001:DB8::/32
2001:DB8::/48
!

Router# show interface tunnel TestIPv4
interface TunnelTestIPv4
 tunnel mode ipv4 decap
 tunnel source direct
 tunnel destination object-group ipv4 Test_IPv4
 no shutdown
!

Router# show interface tunnel TestIPv6
interface TunnelTestIPv6
 tunnel mode ipv6 decap
 tunnel source direct
 tunnel destination object-group ipv6 Test_IPv6
 no shutdown
!
```

### Verification

```

Router# show tunnel ip ea database

----- node0_0_CPU0 -----
tunnel ifhandle 0x80022cc
tunnel source 161.115.1.2
tunnel destination address group Test_IPv4
tunnel transport vrf table id 0xe0000000
tunnel mode gre ipv4, encap
tunnel bandwidth 100 kbps
tunnel platform id 0x0
tunnel flags 0x40003400
IntfStateUp
BcStateUp
Ipv4Caps
Encap
tunnel mtu 1500
tunnel tos 0
tunnel ttl 255
tunnel adjacency flags 0x1
tunnel o/p interface handle 0x0
tunnel key 0x0, entropy length 0 (mask 0xffffffff)
tunnel QT next 0x0
tunnel platform data (nil)
Platform:
Handle: (nil)
Decap ID: 0
Decap RIF: 0
Decap Recycle Encap ID: 0x00000000
Encap RIF: 0
Encap Recycle Encap ID: 0x00000000
Encap IPv4 Encap ID: 0x4001381b
Encap IPv6 Encap ID: 0x00000000
Encap MPLS Encap ID: 0x00000000
DecFEC DecRcyLIF DecStatsId EncRcyLIF

```

## ECMP Hashing Support for Load Balancing

The system inherently supports the n-tuple hash algorithm. The first inner header in the n-tuple hashing includes the source port and the destination port of UDP / TCP protocol headers.

The load balancing performs these functions:

- Incoming data traffic is distributed over multiple equal-cost connections.
- Incoming data traffic is distributed over multiple equal-cost connections member links within a bundle interface.
- Layer 2 bundle and Layer 3 (network layer) load-balancing decisions are taken on IPv4, and IPv6. If it is an IPv4 or an IPv6 payload, then an n-tuple hashing is done.
- An n-tuple hash algorithm provides more granular load balancing and used for load balancing over multiple equal-cost Layer 3 (network layer) paths. The Layer 3 (network layer) path is on a physical interface or on a bundle interface.
- The n-tuple load-balance hash calculation contains:
  - Source IP address
  - Destination IP address

- IP Protocol type
- Router ID
- Source port
- Destination port
- Input interface
- Flow-label (for IPv6 only)

## User-Defined Fields for ECMP Hashing

Table 39: Feature History Table

Feature Name	Release Information	Description
User-Defined Fields for ECMP Hashing	Release 7.5.5	<p>We ensure that in cases where multiple paths are used to carry packets from source to destination, each path is utilized for this purpose and no path is over-utilized or congested. This is made possible because we now provide customized ECMP hashing fields that are used for path computation.</p> <p>Previously, the router relied on fixed packet header fields for hashing, which were not user configurable. With additional user-defined bytes considered for hashing, the granularity at which the traffic can be analyzed for ECMP load balancing increases, resulting in better load balancing and path utilization.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b></p> <ul style="list-style-type: none"> <li>• <b>cef load-balancing fields user-data</b></li> <li>• The <b>show cef exact-route</b> command is modified with a new <b>user-data</b> keyword.</li> <li>• The <b>show cef ipv4 exact-route</b> command is modified with a new <b>user-data</b> keyword.</li> <li>• The <b>show cef ipv6 exact-route</b> command is modified with a new <b>user-data</b> keyword.</li> </ul> <p><b>YANG:</b></p> <ul style="list-style-type: none"> <li>• New Xpath for <code>Cisco-IOS-XR-8000-fib-platform-cfg.yang</code> (see <a href="#">Github</a>, <a href="#">YANG Data Models Navigator</a>).</li> </ul>

ECMP hashing is used to distribute traffic across multiple equal-cost paths. See [ECMP Hashing Support for Load Balancing, on page 222](#) for the default static hashing algorithm details.

You can now add user-defined packet header fields for ECMP path calculation for ipv4 and ipv6 flows using the **cef load-balancing fields user-data** command. Ensure you specify these user-defined fields based on the type of traffic flow that requires load balancing. You can include the following parameters:

- **Hash header:** The hash header specifies which packet header is being considered for load balancing. You can enable any or all of the available six profiles.
  - IPv4: tcp, udp, non-tcp-udp
  - IPv6: tcp, udp, non-tcp-udp

If any hash header profile is defined for load balancing, along with the fixed fields considered for hashing, additional bytes in the payload are also used for path computation.

- **Hashing offset:** The hashing offset specifies the byte location from the end of the configured header.
- **Hash size:** The hash size specifies the number of bytes that is considered from the start of the hash offset by the ECMP hashing algorithm. Range is 1 to 4 bytes.
- **Location:** This specifies the location of the ingress line card that receives the incoming traffic. The user-defined hashing configuration is applied on the specified line card.

The addition of the user-defined packer header fields increases the granularity at which the traffic is analyzed for ECMP load balancing. When multiple paths with equal cost are available for routing a specific type of packet from a source to a destination, this granularity ensures that the intended type of traffic is evenly distributed across these paths. This ensures all available paths are used efficiently and prevents congestion or over-utilization of a single path.

You can also retrieve the exact-route information based on the configured user-data using the **show cef exact-route** command with **user-data** keyword.

**Note**

- When the user-defined hashing configuration is active, any additional options or optional keywords are disregarded during the parsing of incoming packets for retrieving the user-defined bytes.
- The hashing results based on user-defined hash feature is applicable to BGP/IGP ECMP and LAG hashing.
- The use of the user-defined hashing configuration changes the load balancing behavior of GRE and IPinIP traffic. This includes all traffic that begins with ipv4, ipv6, ipv4+udp, ipv6+udp, ipv4+tcp, and ipv6+tcp, regardless of the payload.

## Configure User-Defined Fields for ECMP Hashing

The command **cef load-balancing fields user-data** configures the additional user-defined fields that are to be considered for the hashing algorithm.

This example shows how to configure the additional IPv4 header fields for TCP packets:

```
Router# configure terminal
Router(config)#cef load-balancing fields user-data ipv4 tcp offset 5 size 3 location 0/0/CPU0
Router(config)#commit
```

- offset 5: The payload considered for hashing starts from byte 6 from the end of TCP header.
- size 3: Three bytes of payload are considered.
- location 0/0/CPU0: Specifies the line card on which the configuration is applied.

In the above example, the sixth, seventh, and eighth bytes of the payload are considered additionally for the hashing.

This example shows how to configure the additional IPv6 header fields for UDP packets:

```
Router# configure terminal
Router(config)# cef load-balancing fields user-data ipv6 udp offset 0 size 2 location 0/0/CPU0
Router(config)# commit
```

- offset 0: The payload considered for hashing starts from the end of UDP header.
- size 2: Two bytes of payload are considered.
- location 0/0/CPU0: Specifies the line card on which the configuration is applied.

In the above example, the first two bytes of payload of a UDP packet are considered additionally for the hashing.

## Running Configuration

The following example shows the running configuration:

```
Router# show running-config | include cef
Fri Jul 28 12:02:01.002 UTC
cef load-balancing fields user-data ipv4 tcp offset 5 size 3 location 0/0/CPU0
cef load-balancing fields user-data ipv6 udp offset 0 size 2 location 0/0/CPU0
Router#
```

## Verification

The following example shows the difference in load balancing before and after applying user-defined hashing, for a flow with data that exhibits good hashing behavior.

### Before applying user-defined hashing

```
Router# show interfaces accounting | i IPV6_U
Protocol          Pkts In      Chars In      Pkts Out      Chars Out
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      2            144            0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      0              0            3979416       1981749168
IPV6_UNICAST      4191438       2087336124    0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
IPV6_UNICAST      1             72             0              0
Router#
```

### After applying user-defined hashing

```
Router# show interfaces accounting | i IPV6_U
Protocol          Pkts In      Chars In      Pkts Out      Chars Out
IPV6_UNICAST      0              0              39119         19481262
IPV6_UNICAST      0              0              39801         19820898
IPV6_UNICAST      0              0              40483         20160534
```

IPV6_UNICAST	0	0	40524	20180952
IPV6_UNICAST	0	0	40573	20205354
IPV6_UNICAST	0	0	40614	20225772
IPV6_UNICAST	0	0	39368	19605264
IPV6_UNICAST	0	0	40734	20285532
IPV6_UNICAST	0	0	40777	20306946
IPV6_UNICAST	0	0	40171	20005158
IPV6_UNICAST	0	0	40858	20347284
IPV6_UNICAST	0	0	40269	20053962
IPV6_UNICAST	0	0	41603	20718294
IPV6_UNICAST	0	0	40363	20100774
IPV6_UNICAST	0	0	40407	20122686
IPV6_UNICAST	0	0	41098	20466804
IPV6_UNICAST	850393	423495714	0	0

To view the exact route information allocated to the packets, use **show cef exact-route** command with **user-data** keyword.

The packet contains value 0x2 in the packet position for the ipv6 packet, for which the user-defined configuration has been added for a non-tcp-udp ipv6 flow.

```
Router#show cef ipv6 exact-route 100::10 60::1 flow-label 0 protocol 59 source-port 0
destination-port 0 user-data 0x2 ingress-interface HundredGigE0/0/0/2 location 0/0/cpu0
Unsupported protocol value 59
60::/16, version 1293, internal 0x1000001 0x20 (ptr 0x8b78ef00) [1], 0x400 (0x8e9cfc48),
0x0 (0x0)
Updated Aug 14 07:50:20.022
local adjacency to Bundle-Ether3.30

Prefix Len 16, traffic index 0, precedence n/a, priority 2
via Bundle-Ether3.30
via fe80::72b3:17ff:feae:d703/128, Bundle-Ether3.30, 7 dependencies, weight 0, class 0
[flags 0x0]
path-idx 7 NHID 0x0 [0x8db8bed8 0x0]
next hop fe80::72b3:17ff:feae:d703/128
local adjacency
```







# CHAPTER 15

## Configuring 400G Digital Coherent Optics

Cisco offers a range of the new 400G Digital Coherent QSFP-DD optical modules. The two optical modules that are available are:

- QDD-400G-ZR-S
- QDD-400G-ZRP-S

This chapter describes the QDD-400G-ZR-S, QDD-400G-ZRP-S optical modules and their supported configurations. The following fixed-port routers, line cards, from the indicated Cisco IOS XR software releases, support these two optical modules.

**Table 40: Fixed-Port Routers and Line Cards That Support QDD-400G-ZR-S, QDD-400G-ZRP-S Optical Modules from Indicated Cisco IOS XR Software Releases**

Fixed-Port Routers	Optics PID	Minimum IOS XR Software Release
Cisco 8201	QDD-400G-ZR-S	Release 7.3.15
	QDD-400G-ZRP-S	
Cisco 8202	QDD-400G-ZR-S	Release 7.3.15
	QDD-400G-ZRP-S	
8101-32FH	QDD-400G-ZR-S	Release 7.3.2
	QDD-400G-ZRP-S	
8201-32FH	QDD-400G-ZR-S	Release 7.3.2
	QDD-400G-ZRP-S	
8202-32FH-M	QDD-400G-ZR-S	Release 7.5.2
	QDD-400G-ZRP-S	
Line Cards	Optics PID	Minimum IOS XR Software Release

8800-LC-36FH	QDD-400G-ZR-S	Release 7.3.15
	QDD-400G-ZRP-S	
88-LC0-36FH-M	QDD-400G-ZR-S	Release 7.3.15
	QDD-400G-ZRP-S	
88-LC0-36FH	QDD-400G-ZR-S	Release 7.3.2
	QDD-400G-ZRP-S	
88-LC0-34H14FH	QDD-400G-ZR-S	Release 7.9.1 / Release 7.7.2
	QDD-400G-ZRP-S	



**Note** QDD-400G-ZR-S and QDD-400G-ZRP-S are not supported on 8102-64H fixed-port routers.

QDD-400G-ZRP-S and DP04QSDD-HE0 are not supported on odd-numbered ports of the following routers and line cards:

- Cisco 8201
- Cisco 8202
- 8800-LC-36FH
- 88-LC0-36FH-M

The QDD-400G-ZR-S and QDD-400G-ZRP-S optical modules enable wavelength-division multiplexing (WDM) functionality in the router. These optical modules are DWDM C-band (196.1 THz to 191.3 THz) tunable optical modules. They can be used in both transponder and muxponder modes.

Cisco IOS XR software creates optics and coherent DSP controllers to configure and monitor the performance of the QDD-400G-ZR-S and QDD-400G-ZRP-S optical modules. Optics controllers are used to configure and monitor optical parameters, such as frequency, chromatic dispersion, transmitted output power, modulation, and so on. Coherent DSP controllers are used to monitor network performance parameters like pre- and post-forward error correction (FEC) bit-error rate (pre-FEC BER, post-FEC BER), error corrected bits (EC-BITS), and so on. Forward error correction (FEC) is configured using optical controllers and monitored using coherent DSP controllers.

The QDD-400G-ZR-S and QDD-400G-ZRP-S optical modules support traffic configuration and firmware download. The Cisco IOS XR software collects performance monitoring data and alarms using versatile DOM (VDM).

Due to more power consumption by the QDD-400G-ZR-S and QDD-400G-ZRP-S optical modules, the Cisco IOS XR software operates the fans at a higher speed to cool these optical modules.

The QDD-400G-ZR-S and QDD-400G-ZRP-S optical module configuration is divided into the following categories:

- Traffic configuration – Comprises configuring DAC rate, muxponder mode, modulation, and FEC parameters. Applicable for optics controllers:
  - [Configuring DAC Rate, on page 264](#)

- [Configuring Muxponder Mode, on page 261](#)
- [Configuring Modulation, on page 262](#)
- [Configuring FEC, on page 266](#)
- Optical configuration – Comprises configuring frequency, chromatic dispersion, and optical transmit power. Applicable for optics controllers:
  - [Configuring Frequency, on page 255](#)
  - [Configuring Chromatic Dispersion, on page 257](#)
  - [Configuring Optical Transmit Power, on page 259](#)
- Performance monitoring (PM) – Enables or disables performance monitoring in optical modules. You can also configure PM parameters that comprise signal power, chromatic dispersion, optical signal-to-noise ratio (OSNR), and differential group delay (DGD). Applicable for optics controllers and coherent DSP controllers:
  - [Configuring Performance Monitoring, on page 268](#)
  - [Configuring PM Parameters, on page 268](#)
- Loopback configuration – Configures loopback. Applicable for coherent DSP controller:
  - [Configuring Loopback, on page 267](#)
- Alarms threshold configuration – Configures thresholds for monitoring alarms that include optical signal-to-noise ratio (OSNR), differential group delay (DGD), chromatic dispersion (cd high and low), and so on. Applicable for optics controllers:
  - [Configuring Alarms Threshold, on page 272](#)

The following table contains the possible traffic configuration values for the QDD-400G-ZR-S and QDD-400G-ZRP-S optical modules, in the transponder and muxponder mode:

**Table 41: 400G Digital Coherent QSFP-DD Traffic Configuration Values**

	<b>QDD-400G-ZR-S</b>	<b>QDD-400G-ZRP-S</b>
Client Speed	1x400G, 4x100G	1x400G, 4x100G, 3x100G, 2x100G, 1x100G <b>Note</b> Release 7.3.15 supports only 1x400 and 4x100 client speed.
Trunk Speed	400G	400G, 300G, 200G, 1x100 <b>Note</b> Release 7.3.15 supports only 400G trunk speed.

	<b>QDD-400G-ZR-S</b>	<b>QDD-400G-ZRP-S</b>
Frequency	C-Band, 196.1 To 191.3 THz	C-Band, 196.1 To 191.3 THz
FEC	cFEC	oFEC, cFEC
Modulation	16QAM	16QAM, 8QAM, QPSK Release 7.3.15 supports only 16QAM.
DAC-Rate	1x1	1x1, 1x1.25, 1x1.50
Chromatic Dispersion (CD)	-2400 to +2400	Release 7.3.15: -80000 to +80000 Release 7.3.2: -160000 to +160000
Transmitted (Tx) Power	Each optical module has its own transmitting (TX) power range. You can change the transmitting (TX) power value based on the module capability.	Each optical module has its own transmitting (TX) power optimal values. You can change the transmitting (TX) power value based on the module capability.

#### **QDD-400G-ZR-S Transponder and Muxponder Configuration Values**

The following table contains the possible Transponder and Muxponder configuration values for the QDD-400G-ZR-S optical module:

*Table 42: QDD-400G-ZR-S Transponder and Muxponder Configuration Values*

<b>TXP/MXP</b>	<b>Client</b>	<b>Trunk</b>	<b>Modulation</b>	<b>FEC</b>	<b>DAC Rate</b>
400G-TXP	1 client, 400G speed	1 trunk, 400G	16 QAM	cFEC	1x1
4x100G-MXP	4 clients, 100G speed	1 trunk, 400G	16 QAM	cFEC	1x1

#### **QDD-400G-ZRP-S Transponder and Muxponder Configuration Values**

The following table contains the possible Transponder and Muxponder configuration values for the QDD-400G-ZRP-S optical module:

*Table 43: QDD-400G-ZRP-S Transponder and Muxponder Configuration Values*

<b>TXP/MXP</b>	<b>Client</b>	<b>Trunk</b>	<b>Modulation</b>	<b>FEC</b>	<b>DAC Rate</b>
400G-TXP	1 Client, 400G speed	1 trunk, 400G speed	16 QAM	oFEC	1x1.25
400G-TXP	1 Client, 400G speed	1 trunk, 400G speed	16 QAM	cFEC	1x1

TXP/MXP	Client	Trunk	Modulation	FEC	DAC Rate
4x100G- MXP	4 clients, 100G speed	1 trunk, 400G speed	16 QAM	oFEC	1x1.25
4x100G- MXP	4 clients, 100G speed	1 trunk, 400G speed	16 QAM	cFEC	1x1
3x100G-MXP	3 clients, 100G speed	1 trunk, 400G speed	8 QAM	oFEC	1x1.25
2x100G-MXP	2 clients, 100G speed	1 trunk, 200G speed	QPSK	oFEC	1x1.50
1x100G-MXP	1 client, 100G speed	1 trunk, 100G speed	QPSK	oFEC	1x1.50

- [Configuring Frequency, on page 255](#)
- [Configuring Chromatic Dispersion, on page 257](#)
- [Configuring Optical Transmit Power, on page 259](#)
- [Configuring Muxponder Mode, on page 261](#)
- [Configuring Modulation, on page 262](#)
- [Configuring DAC Rate, on page 264](#)
- [Configuring FEC, on page 266](#)
- [Configuring Loopback, on page 267](#)
- [Configuring Performance Monitoring, on page 268](#)
- [Configuring PM Parameters, on page 268](#)
- [Configuring Alarms Threshold, on page 272](#)

## Configuring Frequency

You can configure frequency on optics controllers. You can select any C band frequency between the range 196.1 to 191.3 THz, in both ITU and NON-ITU channels.



**Note** The 100MHz-grid keyword accepts only frequency values as user input. The 50GHz-grid keyword accepts frequency, ITU-channel, or wavelength values as user input. The Cisco IOS XR software then calculates the frequency for a given wavelength or ITU-channel.

### Frequency Configuration Example

The following example shows how to configure frequency on the optics controller:

```
Router#config
Router(config)#controller optics 0/2/0/16
Router(config-Optics)#dwdm-carrier 100MHz-grid frequency 1921500
Router(config-Optics)#commit
Router(config-Optics)#exit
Router(config)#exit
```

### Running Configuration

This example shows the running configuration:

```
Router#show run controller optics 0/2/0/16
Fri May 28 01:42:32.488 UTC
controller Optics0/2/0/16
  dwdm-carrier 100MHz-grid frequency 1921500
  cd-low-threshold -5000
  cd-high-threshold -5000
!
```

### Verification

This example shows how to verify the frequency configuration:

```
Router#show controller optics 0/2/0/16
Fri May 28 01:47:23.953 UTC
Controller State: Up
Transport Admin State: In Service
Laser State: Off
LED State: Off
FEC State: FEC ENABLED
Optics Status
  Optics Type: QSFPDD 400G ZRP
  DWDM carrier Info: C BAND, MSA ITU Channel=80, Frequency=192.15THz,
  Wavelength=1560.200nm
  Alarm Status:
  -----
  Detected Alarms: None
  LOS/LOL/Fault Status:
  Alarm Statistics:
  -----
  HIGH-RX-PWR = 0           LOW-RX-PWR = 0
  HIGH-TX-PWR = 0           LOW-TX-PWR = 0
  HIGH-LBC = 0             HIGH-DGD = 0
  OOR-CD = 0               OSNR = 0
  WVL-OOL = 0             MEA = 0
  IMPROPER-REM = 0
  TX-POWER-PROV-MISMATCH = 0
  Laser Bias Current = 0.0 mA
  Actual TX Power = -40.00 dBm
  RX Power = -40.00 dBm
  RX Signal Power = -40.00 dBm
  Frequency Offset = 0 MHz
  Laser Temperature = 0.00 Celsius
  Laser Age = 0 %
  DAC Rate = 1x1.25
  Performance Monitoring: Enable
  THRESHOLD VALUES
  -----
  Parameter                High Alarm  Low Alarm  High Warning  Low Warning
  -----
  Rx Power Threshold(dBm)   13.0       -24.0     10.0          -22.0
  Tx Power Threshold(dBm)   0.0        -16.0     -2.0          -14.0
  LBC Threshold(mA)         0.00       0.00     0.00          0.00
  Temp. Threshold(celsius) 80.00      -5.00    75.00         0.00
  Voltage Threshold(volt)   3.46       3.13     3.43          3.16
  LBC High Threshold = 98 %
  Configured Tx Power = -10.00 dBm
  Configured CD High Threshold = -5000 ps/nm
  Configured CD lower Threshold = -5000 ps/nm
  Configured OSNR lower Threshold = 9.00 dB
  Configured DGD Higher Threshold = 80.00 ps
  Baud Rate = 60.1385459900 GBd
  Modulation Type: 16QAM
  Chromatic Dispersion 0 ps/nm
```

```

Configured CD-MIN -26000 ps/nm  CD-MAX 26000 ps/nm
Second Order Polarization Mode Dispersion = 0.00 ps^2
Optical Signal to Noise Ratio = 0.00 dB
Polarization Dependent Loss = 0.00 dB
Polarization Change Rate = 0.00 rad/s
Differential Group Delay = 0.00 ps
Temperature = 21.00 Celsius
Voltage = 3.42 V
Transceiver Vendor Details
  Form Factor           : QSFP-DD
  Optics type           : QSFPDD 400G ZRP
  Name                  : CISCO-ACACIA
  OUI Number            : 7c.b2.5c
  Part Number           : DP04QSDD-E30-19E
  Rev Number            : 10
  Serial Number         : ACA244900GN
  PID                   : QDD-400G-ZRP-S
  VID                   : ES03
  Firmware Version      : 161.06
  Date Code (yy/mm/dd) : 20/12/08
!

```

## Configuring Chromatic Dispersion

You can configure chromatic dispersion on optics controllers. When you configure the maximum and minimum values for chromatic dispersion for any data rate, ensure that the minimum difference between the configured values is equal to or greater than 1000 ps/nm.

The following table lists the default CD search range:

**Table 44: Default CD Search Range**

Muxponder Rate	FEC Value	Default CD Search Range (Min-Max)
400	OFEC	-26000 to +26000
400	CFEC	-2400 to +2400
300	OFEC	-50000 to +50000
200	OFEC	-50000 to +50000
100	OFEC	-80000 to +80000

### Chromatic Dispersion Configuration Example

This example shows how to configure chromatic dispersion on the optics controller:

```

Router#configure
Router(config)#controller optics 0/0/0/13
Router(config-Optics)#cd-max 4000
Router(config-Optics)#cd-min -4000
Router(config-Optics)#commit
Router(config-Optics)#exit
Router(config)#exit

```

### Running Configuration

This example shows the running configuration for the optics controller:

```
Router#show run controller optics 0/0/0/13
Thu May 13 12:24:42.353 UTC
controller Optics0/0/0/13
  cd-min -4000
  cd-max 4000
  !
```

### Verification

This example shows how to verify the configured chromatic dispersion values for the optics controller:

```
Router#show controller optics 0/0/0/13
Controller State: Up
Transport Admin State: In Service
Laser State: On
LED State: Green
FEC State: FEC ENABLED
Optics Status
  Optics Type: QSFPDD 400G ZR
  DWDM carrier Info: C BAND, MSA ITU Channel=61, Frequency=193.10THz,
  Wavelength=1552.524nm
  Alarm Status:
  -----
  Detected Alarms: None
  LOS/LOL/Fault Status:
  Alarm Statistics:
  -----
  HIGH-RX-PWR = 0          LOW-RX-PWR = 0
  HIGH-TX-PWR = 0          LOW-TX-PWR = 0
  HIGH-LBC = 0            HIGH-DGD = 0
  OOR-CD = 0              OSNR = 35
  WV-L-OOL = 0            MEA = 0
  IMPROPER-REM = 0
  TX-POWER-PROV-MISMATCH = 0
  Laser Bias Current = 0.0 %
  Actual TX Power = -7.87 dBm
  RX Power = -8.27 dBm
  RX Signal Power = -8.43 dBm
  Frequency Offset = 130 MHz
  Performance Monitoring: Enable
  THRESHOLD VALUES
  -----
  Parameter                High Alarm  Low Alarm  High Warning  Low Warning
  -----
  Rx Power Threshold(dBm)   1.9        -28.2     0.0          -25.0
  Tx Power Threshold(dBm)   0.0        -15.0     -2.0         -16.0
  LBC Threshold(mA)         0.00       0.00     0.00         0.00
  Temp. Threshold(celsius)  80.00      -5.00     75.00        15.00
  Voltage Threshold(volt)   3.46       3.13     3.43         3.16
  LBC High Threshold = 98 %
  Configured Tx Power = -6.00 dBm
  Configured CD High Threshold = 80000 ps/nm
  Configured CD lower Threshold = -80000 ps/nm
  Configured OSNR lower Threshold = 9.00 dB
  Configured DGD Higher Threshold = 80.00 ps
  Baud Rate = 59.8437500000 GBd
  Modulation Type: 16QAM
  Chromatic Dispersion 0 ps/nm
Configured CD-MIN -4000 ps/nm CD-MAX 4000 ps/nm
  Second Order Polarization Mode Dispersion = 5.00 ps^2
  Optical Signal to Noise Ratio = 36.30 dB
  Polarization Dependent Loss = 0.40 dB
  Polarization Change Rate = 0.00 rad/s
```



```

Differential Group Delay = 4.00 ps
Temperature = 54.00 Celsius
Voltage = 3.37 V
Transceiver Vendor Details
Form Factor           : QSFP-DD
Optics type          : QSFPDD 400G ZR
Name                 : CISCO-ACACIA
OUI Number           : 7c.b2.5c
Part Number          : DP04QSDD-E20-19E
Rev Number           : 10
Serial Number        : ACA2447003L
PID                  : QDD-400G-ZR-S
VID                  : ES03
Firmware Version     : 61.12
Date Code (yy/mm/dd) : 20/12/02

```

## Configuring Optical Transmit Power

You can set the transmit power of the optical signal.

Each QDD-400G-ZR-S and QDD-400G-ZRP-S optical module has its own optical transmit (TX) power range. You can change the optical transmit (TX) power value based on the module capability. For "Transmitter specifications", see the [Cisco 400G Digital Coherent Optics QSFP-DD Optical Modules Data Sheet](#).

1. Release 7.3.15 supports 4x100G muxponder mode or trunk speed.
2. The default optical transmit power (Tx) value is -10 dBm, however with Tx shaping enabled the maximum power in 1x400G, 4x100G, 3x100, 2x100G, and 1x100G modes may be less than -10 dBm.
3. Release 7.3.2 and future releases support 3x100G, 2x100G, and 1x100G muxponder modes or trunk speed.
4. The default optical transmit power (Tx) value is -10 dBm, however with Tx shaping enabled the maximum power in 1x400G, 4x100G, 3x100, 2x100G, and 1x100G modes may be less than -10 dBm.

### Transmitting Power Configuration Example

The following example shows how to configure the optical transmit (TX) power on the optics controller:

```

Router#config
Router(config)#controller optics 0/2/0/16
Router(config-Optics)#transmit-power -125
Router(config-Optics)#commit
Router(config-Optics)#exit
Router(config)#exit

```

### Running Configuration

This example shows the running configuration for the optics controller:

```

Router#show run controller optics 0/2/0/16
Thu May 13 12:52:35.020 UTC
controller Optics0/0/0/1
  cd-min -4000
  cd-max 4000
  transmit-power -125
!
```

### Verification

This example shows how to verify the configured optical transmit power for the optics controller:

```

Router#show controller optics 0/2/0/16
Fri May 28 02:52:06.182 UTC

```

```

Controller State: Up
Transport Admin State: In Service
Laser State: Off
LED State: Off
FEC State: FEC ENABLED
Optics Status
  Optics Type: QSFPDD 400G ZRP
  DWDM carrier Info: C BAND, MSA ITU Channel=80, Frequency=192.15THz,
  Wavelength=1560.200nm
  Alarm Status:
  -----
  Detected Alarms: None
  LOS/LOL/Fault Status:
  Alarm Statistics:
  -----
  HIGH-RX-PWR = 0           LOW-RX-PWR = 0
  HIGH-TX-PWR = 0           LOW-TX-PWR = 0
  HIGH-LBC = 0             HIGH-DGD = 0
  OOR-CD = 0               OSNR = 0
  WVl-OOL = 0              MEA = 0
  IMPROPER-REM = 0
  TX-POWER-PROV-MISMATCH = 0
  Laser Bias Current = 0.0 mA
  Actual TX Power = -40.00 dBm
  RX Power = -40.00 dBm
  RX Signal Power = -40.00 dBm
  Frequency Offset = 0 MHz
  Laser Temperature = 0.00 Celsius
  Laser Age = 0 %
  DAC Rate = 1x1.25
  Performance Monitoring: Enable
  THRESHOLD VALUES
  -----
  Parameter                High Alarm  Low Alarm  High Warning  Low Warning
  -----
  Rx Power Threshold(dBm)   13.0       -24.0      10.0          -22.0
  Tx Power Threshold(dBm)   0.0        -16.0      -2.0          -14.0
  LBC Threshold(mA)         0.00       0.00      0.00          0.00
  Temp. Threshold(celsius)  80.00     -5.00     75.00         0.00
  Voltage Threshold(volt)   3.46       3.13      3.43          3.16
  LBC High Threshold = 98 %
  Configured Tx Power = -12.50 dBm
  Configured CD High Threshold = -5000 ps/nm
  Configured CD lower Threshold = -5000 ps/nm
  Configured OSNR lower Threshold = 9.00 dB
  Configured DGD Higher Threshold = 80.00 ps
  Baud Rate = 60.1385459900 GBd
  Modulation Type: 16QAM
  Chromatic Dispersion 0 ps/nm
  Configured CD-MIN -4000 ps/nm CD-MAX 4000 ps/nm
  Second Order Polarization Mode Dispersion = 0.00 ps^2
  Optical Signal to Noise Ratio = 0.00 dB
  Polarization Dependent Loss = 0.00 dB
  Polarization Change Rate = 0.00 rad/s
  Differential Group Delay = 0.00 ps
  Temperature = 20.00 Celsius
  Voltage = 3.41 V
Transceiver Vendor Details
  Form Factor                : QSFP-DD
  Optics type                 : QSFPDD 400G ZRP
  Name                       : CISCO-ACACIA
  OUI Number                  : 7c.b2.5c
  Part Number                  : DP04QSDD-E30-19E
  Rev Number                   : 10

```

```

Serial Number      : ACA244900GN
PID               : QDD-400G-ZRP-S
VID              : ES03
Firmware Version  : 161.06
Date Code (yy/mm/dd) : 20/12/08

```

## Configuring Muxponder Mode

By default, the Cisco IOS XR software configures the QDD-400G-ZR-S and QDD-400G-ZRP-S optical modules in the 400G transponder mode.

Using the **breakout muxponder mode** command, you can configure muxponder mode on optics controllers. Based on the muxponder mode, you can choose the modulation.

Muxponder mode options available for QDD-400G-ZR-S are:

- 4x100

Muxponder mode options available for QDD-400G-ZRP-S are:

- 4x100
- 3x100
- 2x100




---

**Note** Release 7.3.15 supports only 4x100 muxponder mode.

---

See the following tables for the modulation values, based on the muxponder mode:

- [QDD-400G-ZR-S Transponder and Muxponder Configuration Values, on page 254](#)
- [QDD-400G-ZRP-S Transponder and Muxponder Configuration Values, on page 254](#)

Using the **no breakout muxponder mode** command, you can switch from the muxponder mode to the transponder mode, on optics controllers.

### Muxponder Mode Configuration Example

The following example shows how to configure muxponder mode on the optics controller:

```

Router#config
Router(config)#controller optics 0/0/0/13
Router(config-Optics)#breakout 4x100
Router(config-Optics)#commit
Router(config-Optics)#exit
Router(config)#exit

```




---

**Note** In the above example, the Cisco IOS XR software creates four Ethernet clients with 100GE speed, which can be verified using the **show interfaces brief | include R/S/I/P** command.

---

### Running Configuration

This example shows the running configuration for the optics controller:

```
Router#show run controller optics 0/0/0/13
Thu May 13 12:24:42.353 UTC
controller Optics0/0/0/13
  cd-min -4000
  cd-max 4000
  breakout 4x100
  !
```

### Verification

This example shows how to verify the muxponder mode configuration:

```
Router#show interfaces brief | include 0/0/0/13
Hu0/0/0/13/0          up          up          ARPA  1514  100000000
Hu0/0/0/13/1          up          up          ARPA  1514  100000000
Hu0/0/0/13/2          up          up          ARPA  1514  100000000
Hu0/0/0/13/3          up          up          ARPA  1514  100000000
```

### Transponder Mode Configuration Example

The following example shows how to switch to the transponder mode, on the optics controller:

```
Router#config
Router(config)#controller optics 0/0/0/13
Router(config-Optics)#no breakout 4x100
Router(config-Optics)#commit
Router(config-Optics)#exit
Router(config)#exit
```




---

**Note** The Cisco IOS XR software creates a single 400GE interface, which can be verified using the **show interfaces brief | include R/S/I/P** command.

---

### Running Configuration

This example shows the running configuration for the optics controller. The breakout configuration is absent in the running configuration.

```
Router#show run controller optics 0/0/0/13
Thu May 13 13:51:20.330 UTC
controller Optics0/0/0/13
  cd-min -4000
  cd-max 4000
  transmit-power -100
  !
```

### Verification

This example shows how to verify the transponder mode configuration:

```
Router#show interfaces brief | include 0/0/0/13
FH0/0/0/13          up          up          ARPA  1514  400000000
```

## Configuring Modulation

You can configure modulation on optics controllers. Based on the muxponder mode, you can choose the modulation.



**Note** The system accepts any modulation value that is entered. However, if the modulation value is outside the supported range, it is not configured on the optical module. Instead, the optical module is auto-configured with a valid modulation value. To view this value, use the **show controller optics R/S/I/P** command.

See the following tables for the supported modulation values:

- [QDD-400G-ZR-S Transponder and Muxponder Configuration Values, on page 254](#)
- [QDD-400G-ZRP-S Transponder and Muxponder Configuration Values, on page 254](#)

### Modulation Configuration Example

The following example shows how to configure modulation on the optics controller:

```
Router#config
Router(config)#controller optics 0/0/0/1
Router(config-Optics)#modulation 16Qam
Router(config-Optics)#commit
Router(config-Optics)#exit
Router(config)#exit
```

### Running Configuration

This example shows the running configuration:

```
Router#show run controller optics 0/0/0/1
controller Optics0/0/0/1
  cd-min -4000
  cd-max 4000
  transmit-power -100
  modulation 16Qam
!
```



**Note** Use the **show controller optics R/S/I/P** command to verify the modulation value of the optical module.

### Verification

This example shows how to verify the configured modulation value for the optics controller:

```
Router#show controller optics 0/0/0/1
Controller State: Up
Transport Admin State: In Service
Laser State: On
LED State: Green
FEC State: FEC ENABLED
Optics Status
  Optics Type: QSPDD 400G ZR
  DWDM carrier Info: C BAND, MSA ITU Channel=61, Frequency=193.10THz,
  Wavelength=1552.524nm
  Alarm Status:
  -----
  Detected Alarms: None
  LOS/LOL/Fault Status:
  Alarm Statistics:
  -----
  HIGH-RX-PWR = 0          LOW-RX-PWR = 0
  HIGH-TX-PWR = 0          LOW-TX-PWR = 0
  HIGH-LBC = 0            HIGH-DGD = 0
```

```

OOR-CD = 0                OSNR = 35
WVL-OOL = 0              MEA = 0
IMPROPER-REM = 0
TX-POWER-PROV-MISMATCH = 0
Laser Bias Current = 0.0 %
Actual TX Power = -7.87 dBm
RX Power = -8.27 dBm
RX Signal Power = -8.43 dBm
Frequency Offset = 130 MHz
Performance Monitoring: Enable
THRESHOLD VALUES
-----
Parameter                High Alarm  Low Alarm  High Warning  Low Warning
-----
Rx Power Threshold(dBm)   1.9        -28.2     0.0          -25.0
Tx Power Threshold(dBm)  0.0        -15.0     -2.0         -16.0
LBC Threshold(mA)        0.00       0.00     0.00         0.00
Temp. Threshold(celsius) 80.00      -5.00     75.00        15.00
Voltage Threshold(volt)  3.46       3.13     3.43         3.16
LBC High Threshold = 98 %
Configured Tx Power = -6.00 dBm
Configured CD High Threshold = 80000 ps/nm
Configured CD lower Threshold = -80000 ps/nm
Configured OSNR lower Threshold = 9.00 dB
Configured DGD Higher Threshold = 80.00 ps
Baud Rate = 59.8437500000 GBd
Modulation Type: 16QAM
Chromatic Dispersion 0 ps/nm
Configured CD-MIN -4000 ps/nm CD-MAX 4000 ps/nm
Second Order Polarization Mode Dispersion = 5.00 ps^2
Optical Signal to Noise Ratio = 36.30 dB
Polarization Dependent Loss = 0.40 dB
Polarization Change Rate = 0.00 rad/s
Differential Group Delay = 4.00 ps
Temperature = 54.00 Celsius
Voltage = 3.37 V
Transceiver Vendor Details
Form Factor                : QSFP-DD
Optics type                 : QSFPDD 400G ZR
Name                       : CISCO-ACACIA
OUI Number                 : 7c.b2.5c
Part Number                 : DP04QSDD-E20-19E
Rev Number                 : 10
Serial Number               : ACA2447003L
PID                        : QDD-400G-ZR-S
VID                        : ES03
Firmware Version           : 61.12
Date Code(yy/mm/dd)        : 20/12/02

```

## Configuring DAC Rate

You can set the DAC (digital to analog conversion) sampling rate on optics controllers. You can modify the DAC sampling rate only on the QDD-400G-ZRP-S optical module.



**Note** QDD-400G-ZR-S supports 1x1 dac-rate in cFEC mode. QDD-400G-ZRP-S supports 1x1 dac-rate in cFEC mode and 1x1.25 dac-rate in oFEC mode.

### DAC Rate Configuration Example

The following example shows how to set the DAC rate on the optics controller:

```
Router#config
Router(config)#controller optics 0/0/0/1
Router(config-Optics)#dac-rate 1x1
```

### Verification

This example shows the running configuration:

```
Router#show run controller optics 0/0/0/1
Thu May 13 12:52:35.020 UTC
controller Optics0/0/0/1
  cd-min -4000
  cd-max 4000
  transmit-power -100
  modulation 16Qam
  DAC-Rate 1x1
!
```

### Verification

This example shows how to verify the configured DAC rate for the optics controller:

```
Router#show controller optics 0/0/0/1
Controller State: Up
Transport Admin State: In Service
Laser State: On
LED State: Green
FEC State: FEC ENABLED
Optics Status
  Optics Type: QSPDD 400G ZR
  DWDM carrier Info: C BAND, MSA ITU Channel=61, Frequency=193.10THz,
  Wavelength=1552.524nm
  Alarm Status:
  -----
  Detected Alarms: None
  LOS/LOL/Fault Status:
  Alarm Statistics:
  -----
  HIGH-RX-PWR = 0          LOW-RX-PWR = 0
  HIGH-TX-PWR = 0          LOW-TX-PWR = 0
  HIGH-LBC = 0             HIGH-DGD = 0
  OOR-CD = 0               OSNR = 35
  WVL-OOL = 0              MEA = 0
  IMPROPER-REM = 0
  TX-POWER-PROV-MISMATCH = 0
  Laser Bias Current = 0.0 %
  Actual TX Power = -7.87 dBm
  RX Power = -8.27 dBm
  RX Signal Power = -8.43 dBm
  Frequency Offset = 130 MHz
  DAC Rate = 1x1
  Performance Monitoring: Enable
  THRESHOLD VALUES
  -----
  Parameter                High Alarm  Low Alarm  High Warning  Low Warning
  -----
  Rx Power Threshold(dBm)   1.9         -28.2      0.0           -25.0
  Tx Power Threshold(dBm)   0.0         -15.0      -2.0          -16.0
  LBC Threshold(mA)         0.00        0.00       0.00          0.00
  Temp. Threshold(celsius)  80.00       -5.00      75.00         15.00
  Voltage Threshold(volt)   3.46        3.13       3.43          3.16
  LBC High Threshold = 98 %
```

```

Configured Tx Power = -6.00 dBm
Configured CD High Threshold = 80000 ps/nm
Configured CD lower Threshold = -80000 ps/nm
Configured OSNR lower Threshold = 9.00 dB
Configured DGD Higher Threshold = 80.00 ps
Baud Rate = 59.8437500000 GBd
Modulation Type: 16QAM
Chromatic Dispersion 0 ps/nm
Configured CD-MIN -4000 ps/nm CD-MAX 4000 ps/nm
Second Order Polarization Mode Dispersion = 5.00 ps^2
Optical Signal to Noise Ratio = 36.30 dB
Polarization Dependent Loss = 0.40 dB
Polarization Change Rate = 0.00 rad/s
Differential Group Delay = 4.00 ps
Temperature = 54.00 Celsius
Voltage = 3.37 V
Transceiver Vendor Details
Form Factor           : QSFP-DD
Optics type           : QSFPDD 400G ZR
Name                  : CISCO-ACACIA
OUI Number            : 7c.b2.5c
Part Number           : DP04QSDD-E20-19E
Rev Number            : 10
Serial Number         : ACA2447003L
PID                   : QDD-400G-ZR-S
VID                   : ES03
Firmware Version      : 61.12
Date Code (yy/mm/dd) : 20/12/02

```

## Configuring FEC

You can configure forward error correction (FEC) only on optics controllers. You can modify FEC only on the QDD-400G-ZRP-S optical module. FEC is a feature that is used for controlling errors during data transmission. This feature works by adding data redundancy to the transmitted message using an algorithm. This redundancy allows the receiver to detect and correct a limited number of errors occurring anywhere in the message, instead of having to ask the transmitter to resend the message.




---

**Note** QDD-400G-ZR-S supports cFEC (concatenated forward error correction). QDD-400G-ZRP-S supports cFEC and oFEC (open forward error correction).

---

### FEC Configuration Example

The following sample shows how to configure FEC on the optics controller:

```

Router#configure
Router(config)#controller optics 0/0/0/13
Router(config-Optics)#fec CFEC
Router(config-Optics)#commit
Router(config-Optics)#exit
Router(config)#exit

```

### Running Configuration

This example shows the running configuration:

```

Router#show controllers optics 0/0/0/13
controller Optics0/0/0/1
cd-min -4000

```



```

cd-max 4000
transmit-power -100
fec CFEC
modulation 16Qam
DAC-Rate 1x1.25
!

```

### Verification

This example shows how to verify the FEC configuration for the optics controller:

```

Router#show controller coherentdsp 0/0/0/13
Thu May 27 17:28:51.960 UTC
Port                               : CoherentDSP 0/0/0/13
Controller State                   : Down
Inherited Secondary State         : Normal
Configured Secondary State       : Maintenance
Derived State                      : Maintenance
Loopback mode                     : Internal
BER Thresholds                    : SF = 1.0E-5  SD = 1.0E-7
Performance Monitoring            : Enable
Bandwidth                         : 400.0Gb/s

Alarm Information:
LOS = 6 LOF = 0 LOM = 0
OOF = 0 OOM = 0 AIS = 0
IAE = 0 BIAE = 0          SF_BER = 0
SD_BER = 0          BDI = 0 TIM = 0
FECMISMATCH = 0 FEC-UNC = 0      FLEXO_GIDM = 0
FLEXO-MM = 0      FLEXO-LOM = 0  FLEXO-RDI = 0
FLEXO-LOF = 5
Detected Alarms                   : LOS
Bit Error Rate Information
PREFEC BER                        : 5.0E-01
POSTFEC BER                       : 0.0E+00
Q-Factor                          : 0.00 dB
Q-Margin                          : -7.20dB
OTU TTI Received

FEC mode                         : C_FEC

```

## Configuring Loopback

You can configure internal or line loopback on coherent DSP controllers. Loopback can be performed only in the maintenance mode.

### Loopback Configuration Example

This example shows how to enable internal loopback configuration on coherent DSP controllers:

```

Router#config
Router(config)#controller coherentDSP 0/0/0/4
Router(config-CoDSP)#secondary-admin-state maintenance
Router(config-CoDSP)#loopback internal
Router(config-CoDSP)#commit

```

### Running Configuration

This example shows the running configuration on coherent DSP controllers:

```

Router#show run controller coherentdsp 0/0/0/4
Thu May 13 19:51:08.175 UTC
controller CoherentDSP0/0/0/4

```

```

secondary-admin-state maintenance
loopback internal
!

```

### Verification

This example shows how to verify the loopback configuration on coherent DSP controllers:

```

Router#show controller coherentdsp 0/0/0/4
Thu May 27 17:28:51.960 UTC
Port                               : CoherentDSP 0/0/0/4
Controller State                   : Down
Inherited Secondary State          : Normal
Configured Secondary State       : Maintenance
Derived State                      : Maintenance
Loopback mode                   : Internal
BER Thresholds                    : SF = 1.0E-5  SD = 1.0E-7
Performance Monitoring             : Enable
Bandwidth                          : 400.0Gb/s
Alarm Information:
LOS = 6 LOF = 0 LOM = 0
OOF = 0 OOM = 0 AIS = 0
IAE = 0 BIAE = 0          SF_BER = 0
SD_BER = 0          BDI = 0 TIM = 0
FECMISMATCH = 0 FEC-UNC = 0          FLEXO_GIDM = 0
FLEXO-MM = 0          FLEXO-LOM = 0  FLEXO-RDI = 0
FLEXO-LOF = 5
Detected Alarms                   : LOS
Bit Error Rate Information
PREFEC BER                        : 5.0E-01
POSTFEC BER                       : 0.0E+00
Q-Factor                          : 0.00 dB
Q-Margin                          : -7.20dB
OTU TTI Received
FEC mode                           : C_FEC

```

## Configuring Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for, and report performance data for early detection of problems. The user can retrieve both current and historical PM counters for the various controllers in 30-second, 15-minute, and 24-hour intervals.

Performance monitoring can be configured on optics controllers and coherent DSP controllers.

To stop performance monitoring on optics or coherent DSP controllers, use the **perf-mon disable** keyword.

## Configuring PM Parameters

The performance monitoring (PM) threshold and the threshold crossing alert (TCA) reporting status can be configured for optics controllers and coherent DSP controllers:

**Table 45: PM Thresholds and TCA Report Status for Optics Controllers**

PM Parameters	Description
CD	Sets the CD (chromatic dispersion) threshold or TCA reporting status.

PM Parameters	Description
DGD	Sets the DGD (differential group delay) threshold or TCA reporting status.
LBC	Sets the LBC (laser bias current) threshold or TCA reporting status in mA.
FREQ-OFF	Sets the FREQ-OFF (low signal frequency offset) threshold or TCA reporting status in Mhz.
OPR	Sets the OPR (optical power RX) threshold or TCA reporting status in uW or dbm.
OPT	Sets the OPT (optical power TX) threshold or TCA reporting status in uW or dbm.
OSNR	Sets the OSNR (optical signal-to-noise ratio) threshold or TCA reporting status.
PCR	Sets the PCR (polarization change rate) threshold or TCA reporting status.
PDL	Sets the PDL (polarization dependent loss) threshold or TCA reporting status.
RX-SIG	Sets the RX-SIG (receiving signal power) threshold or TCA reporting status in uW or dbm.
SNR	Sets the SNR (signal-to-noise ratio) threshold or TCA reporting status.
SOPMD	Sets the SOPMD (second order polarization mode dispersion) threshold or TCA reporting status.

**Table 46: PM Thresholds TCA Report Status for Coherent DSP Controllers**

PM Parameters	Description
Q	Sets the Q threshold or TCA reporting status.
Q-margin	Sets the Q margin threshold or TCA reporting status.
EC-BITS	Sets the EC-BITS (error corrected bits) threshold or TCA reporting status.
PostFEC BER	Sets the post-FEC BER threshold or TCA reporting status.
PreFEC BER	Sets the pre-FEC BER threshold or TCA reporting status.
UC-WORDS	Sets the UC-WORDS (uncorrected words) threshold or TCA reporting status.

PM Parameters	Description
Host-Intf-0-FEC-BER	<p>Sets the Host-Intf-0-FEC-BER threshold or TCA reporting status, where:</p> <ul style="list-style-type: none"> <li>• AVG - specifies the number of corrected bits received from the host interface prior to a PM interval.</li> <li>• MIN - specifies the minimum number of corrected bits received from the host interface over a sub-interval and prior to a PM interval.</li> <li>• MAX - specifies the maximum number of corrected bits received from the host interface over a sub-interval and prior to a PM interval.</li> </ul>
Host-Intf-0-FEC-FERC	<p>Sets the Host-Intf-0-FEC-FERC threshold or TCA reporting status, where:</p> <ul style="list-style-type: none"> <li>• AVG - specifies the number of frames received from the host interface during a sub-interval.</li> <li>• MIN - specifies the minimum number of frames received from the host interface with uncorrected errors over a sub-interval and prior to a PM interval.</li> <li>• MAX - specifies the maximum number of frames received from the host interface with uncorrected errors over a sub-interval and prior to a PM interval.</li> </ul>

### Performance Monitoring Configuration Example

This example shows how to enable performance monitoring and set PM thresholds on the optics controller:

```
Router#config
Router(config)#controller optics 0/2/0/16
Router(config-Optics)#perf-mon enable
Router(config-Optics)#pm 30-sec optics threshold cd max 100
Router(config-Optics)#pm 30-sec optics threshold cd min -100
Router(config-Optics)#commit
```

### Running Configuration

This example shows the running configuration on optics controllers:

```
Router#show run controller optics 0/2/0/16
Thu May 13 20:18:55.957 UTC
controller Optics0/2/0/16
pm 30-sec optics threshold cd max 100
pm 30-sec optics threshold cd min -100
perf-mon enable
!
```

### Verification

This example shows how to verify the PM parameters on optics controllers. Verify the configuration changes in the Configured Threshold fields:

```
Router#show controller optics 0/2/0/16 pm current 30-sec optics 1
Thu May 27 17:58:49.889 UTC
Optics in the current interval [17:58:30 - 17:58:49 Thu May 27 2021]
Optics current bucket type : Valid
```

	MIN	AVG	MAX	Operational	Configured	TCA	Operational
Configured		TCA		Threshold(min)	Threshold(min)	(min)	Threshold(max)
LBC[ <b>mA</b> ]	: 0.0	0.0	0.0	0.0	NA	NO	100.0
NA		NO					
OPT[ <b>dBm</b> ]	: -9.98	-9.98	-9.98	-15.09	NA	NO	0.00
NA		NO					
OPR[ <b>dBm</b> ]	: -40.00	-40.00	-40.00	-30.00	NA	NO	8.00
NA		NO					
CD[ <b>ps/nm</b> ]	: 0	0	0	-80000	<b>-100</b>	NO	100
<b>100</b>		NO					
DGD[ <b>ps</b> ]	: 0.00	0.00	0.00	0.00	NA	NO	80.00
NA		NO					
SOPMD[ <b>ps^2</b> ]	: 0.00	0.00	0.00	0.00	NA	NO	2000.00
NA		NO					
OSNR[ <b>dB</b> ]	: 0.00	0.00	0.00	0.00	NA	NO	40.00
NA		NO					
PDL[ <b>dB</b> ]	: 0.00	0.00	0.00	0.00	NA	NO	7.00
NA		NO					
PCR[ <b>rad/s</b> ]	: 0.00	0.00	0.00	0.00	NA	NO	2500000.00
NA		NO					
RX_SIG[ <b>dBm</b> ]	: -40.00	-40.00	-40.00	-30.00	NA	NO	1.00
NA		NO					
FREQ_OFF[ <b>Mhz</b> ]	: 0	0	0	-3600	NA	NO	3600
NA		NO					
SNR[ <b>dB</b> ]	: 0.00	0.00	0.00	7.00	NA	NO	100.00
NA		NO					

```
Last clearing of "show controllers OPTICS" counters never
!
```

### Performance Monitoring Configuration Example

This example shows how to enable performance monitoring and set PM thresholds and TCA reporting status on the coherent DSP controller:

```
Router#config
Router(config)#controller CoherentDSP0/2/0/16
Router(config-CoDSP)#perf-mon enable
Router(config-CoDSP)#pm 30-sec fec report Q max-tca enable
Router(config-CoDSP)#pm 30-sec fec report Q-margin max-tca enable
Router(config-CoDSP)#pm 30-sec fec report Q min-tca enable
Router(config-CoDSP)#pm 30-sec fec report Q-margin min-tca enable
Router(config-CoDSP)#pm 30-sec fec threshold Q max 1200
Router(config-CoDSP)#pm 30-sec fec threshold Q-margin max 500
Router(config-CoDSP)#pm 30-sec fec threshold Q min 900
Router(config-CoDSP)#pm 30-sec fec threshold Q-margin min 280
Router(config-CoDSP)#commit
```

### Running Configuration

This example shows the running configuration on coherent DSP controllers:

```
Router#show run controller coherentdsp 0/2/0/16
Thu May 13 19:56:09.136 UTC
controller CoherentDSP0/2/0/16
  pm 30-sec fec report Q max-tca enable
```

```

pm 30-sec fec report Q-margin max-tca enable
pm 30-sec fec report Q min-tca enable
pm 30-sec fec report Q-margin min-tca enable
pm 30-sec fec threshold Q max 1200
pm 30-sec fec threshold Q-margin max 500
pm 30-sec fec threshold Q min 900
pm 30-sec fec threshold Q-margin min 280
perf-mon enable
!

```

### Verification

This example shows how to verify the PM parameters on coherent DSP controllers. Verify the configuration changes in the highlighted fields:

```

Router#show controllers coherentdsp 0/2/0/16 pm current 30-sec fec
Thu May 27 23:04:54.167 UTC
g709 FEC in the current interval [23:04:30 - 23:04:54 Thu May 27 2021]
FEC current bucket type : Valid
  EC-BITS      : 0                      Threshold : 111484000000          TCA(enable)  :
YES
  UC-WORDS    : 0                      Threshold : 5                      TCA(enable)  :
YES

```

Threshold	TCA	MIN	AVG	MAX	Threshold	TCA
(max)	(enable)				(min)	(enable)
PreFEC BER		0E-15	0E-15	0E-15	0E-15	NO
0E-15	NO					
PostFEC BER		0E-15	0E-15	0E-15	0E-15	NO
0E-15	NO					
Q[dB]		0.00	0.00	0.00	<b>9.00</b>	<b>YES</b>
Q_Margin[dB]		0.00	0.00	0.00	<b>2.80</b>	<b>YES</b>
					<b>120.00</b>	<b>YES</b>
					<b>5.00</b>	<b>YES</b>

```

!

```

## Configuring Alarms Threshold

The alarms threshold can be configured for monitoring alarms on optics controllers:

**Table 47: Alarms Threshold Parameters for Optics Controllers**

Alarm Threshold Parameters	Description
CD	Sets the CD (chromatic dispersion) alarm threshold (cd-low-threshold and cd-high-threshold).
DGD	Sets the DGD (differential group delay) alarm threshold.
LBC	Sets the LBC (laser bias current) threshold in mA.
OSNR	Sets the OSNR (optical signal-to-noise ratio) alarm threshold.

### Alarm Threshold Configuration Example

This example shows how to configure alarm threshold on the optics controller:

```
Router#config
Router(config)#controller optics 0/2/0/16
Router(config-Optics)#cd-low-threshold -2000
Router(config-Optics)#cd-high-threshold 2000
Router(config-Optics)#commit
```

### Running Configuration

This example shows the running configuration on the optics controller:

```
Router#show run controller optics 0/2/0/16
Thu May 13 20:18:55.957 UTC
controller Optics0/2/0/16
  cd-low-threshold 2000
  cd-high-threshold 2000
!
```

### Verification

This example shows how to verify the alarm threshold on optics controllers:

```
Router#show controller optics 0/2/0/16
Fri May 28 01:04:33.604 UTC
Controller State: Up
Transport Admin State: In Service
Laser State: Off
LED State: Off
FEC State: FEC ENABLED
Optics Status
  Optics Type: QSFPDD 400G ZRP
  DWDM carrier Info: C BAND, MSA ITU Channel=61, Frequency=193.10THz,
  Wavelength=1552.524nm
  Alarm Status:
  -----
  Detected Alarms: None
  LOS/LOL/Fault Status:
  Alarm Statistics:
  -----
  HIGH-RX-PWR = 0          LOW-RX-PWR = 0
  HIGH-TX-PWR = 0          LOW-TX-PWR = 0
  HIGH-LBC = 0            HIGH-DGD = 0
  OOR-CD = 0              OSNR = 0
  WVl-OOL = 0             MEA = 0
  IMPROPER-REM = 0
  TX-POWER-PROV-MISMATCH = 0
  Laser Bias Current = 0.0 mA
  Actual TX Power = -40.00 dBm
  RX Power = -40.00 dBm
  RX Signal Power = -40.00 dBm
  Frequency Offset = 0 MHz
  Laser Temperature = 0.00 Celsius
  Laser Age = 0 %
  DAC Rate = 1x1.25
  Performance Monitoring: Enable
  THRESHOLD VALUES
  -----
  Parameter                High Alarm  Low Alarm  High Warning  Low Warning
  -----
  Rx Power Threshold(dBm)   13.0       -24.0      10.0          -22.0
  Tx Power Threshold(dBm)   0.0        -16.0      -2.0          -14.0
  LBC Threshold(mA)         0.00       0.00      0.00          0.00
  Temp. Threshold(celsius)  80.00     -5.00     75.00         0.00
  Voltage Threshold(volt)   3.46       3.13      3.43          3.16
  LBC High Threshold = 98 %
  Configured Tx Power = -10.00 dBm
```

```

Configured CD High Threshold = -5000 ps/nm
Configured CD lower Threshold = -5000 ps/nm
Configured OSNR lower Threshold = 9.00 dB
Configured DGD Higher Threshold = 80.00 ps
Baud Rate = 60.1385459900 GBd
Modulation Type: 16QAM
Chromatic Dispersion 0 ps/nm
Configured CD-MIN -26000 ps/nm CD-MAX 26000 ps/nm
Second Order Polarization Mode Dispersion = 0.00 ps^2
Optical Signal to Noise Ratio = 0.00 dB
Polarization Dependent Loss = 0.00 dB
Polarization Change Rate = 0.00 rad/s
Differential Group Delay = 0.00 ps
Temperature = 21.00 Celsius
Voltage = 3.42 V

```

## Transceiver Vendor Details

```

Form Factor           : QSFP-DD
Optics type           : QSFPDD 400G ZRP
Name                  : CISCO-ACACIA
OUI Number            : 7c.b2.5c
Part Number           : DP04QSDD-E30-19E
Rev Number            : 10
Serial Number         : ACA244900GN
PID                   : QDD-400G-ZRP-S
VID                   : ES03
Firmware Version      : 161.06
Date Code(yy/mm/dd)  : 20/12/08

```

!





## CHAPTER 16

# Configuring Controllers

This chapter describes the Optics Controller for the 36-port QSFP56-DD 400 GbE and 48-port QSFP28 100 GbE Line Cards. This chapter also describes the procedures used to configure the controllers.



---

**Note** When two MACsec enabled Cisco 8000 Series Routers with Coherent Line Cards are connected, there is no compatibility between Coherent Line Cards of IOS XR Release.

---

Following controller configuration options are supported on the router:

- breakout - Configure breakout mode ('breakout 4x10' only.)
- clear - Clear the uncommitted configuration.
- commit - Commit the configuration changes to running.
- do - Run an exec command.
- end - Exit from configure mode.
- exit - Exit from this submode.
- ext-description - Set ext-description for this controller.
- no - Negate a command or set its defaults.
- pwd - Commands used to reach current submode.
- root - Exit to the global configuration mode.
- show - Show contents of configuration.
  
- [How to Configure Controllers, on page 276](#)
- [Diagnostic Parameters for Optical Transceivers, on page 279](#)
- [Loopback on Optical Transceivers, on page 285](#)
- [Media Side Input Loopback Configuration, on page 287](#)
- [Media Side Output Loopback, on page 288](#)
- [Host Side Input Loopback Configuration, on page 289](#)
- [Host Side Output Loopback Configuration, on page 291](#)

# How to Configure Controllers

This section contains the following procedures:

## Configuring Optics Controller

Configuring optics controller of breakout 4x10:

```
RP/0/RP0/CPU0:uut#configure
Fri Oct 11 16:22:31.222 UTC
RP/0/RP0/CPU0:uut(config)#controller optics 0/1/0/28
RP/0/RP0/CPU0:uut(config-Optics)#breakout 4x10
RP/0/RP0/CPU0:uut(config-Optics)#commit
Fri Oct 11 16:23:26.868 UTC
RP/0/RP0/CPU0:uut(config-Optics)#end
RP/0/RP0/CPU0:uut#
RP/0/RP0/CPU0:uut#show running-config controller optics 0/1/0/28
Fri Oct 11 16:23:41.273 UTC
controller Optics0/1/0/28
breakout 4x10
!
```

## Disabling Optical Modules

This feature provides the ability to disable and re-enable an optical module through CLI, which simulates online insertion and removal (OIR) by disabling power to the transceiver port.

Typical troubleshooting procedures for optical modules can include performing OIR by removing and re-installing the module, which requires onsite personnel to physically reseal the optical module. The ability to remotely disable and enable an optical module can significantly reduce operational expenses.

### Example

The following output shows a QSFP28 module powered on and in UP state:

```
Router# show controllers optics 0/0/0/0

Controller State: Up

Transport Admin State: In Service

Laser State: Off

LED State: Not Applicable

FEC State: FEC ENABLED

Optics Status

    Optics Type: QSFP28 100G FR
    Wavelength = 1311.00 nm

    Alarm Status:
    -----
    Detected Alarms: None
```

LOS/LOL/Fault Status:

Laser Bias Current = 26.2 mA  
 Actual TX Power = 0.73 dBm  
 RX Power = -0.68 dBm

Performance Monitoring: Disable

THRESHOLD VALUES

-----

Parameter	High Alarm	Low Alarm	High Warning	Low Warning
Rx Power Threshold(dBm)	7.4	-10.4	4.5	-6.3
Tx Power Threshold(dBm)	7.0	-6.3	4.0	-2.4
LBC Threshold(mA)	100.00	8.00	83.00	10.00
Temp. Threshold(celsius)	75.00	-5.00	70.00	0.00
Voltage Threshold(volt)	3.63	2.97	3.46	3.13

Polarization parameters not supported by optics

Temperature = 27.92 Celsius  
 Voltage = 3.24 V

Transceiver Vendor Details

```

Form Factor           : QSFP28
Optics type           : QSFP28 100G FR
Name                  : CISCO-CISCO
OUI Number            : 00.00.0c
Part Number           : 10-3248-01
Rev Number            : 01
Serial Number         : FBN2331A114
PID                   : QSFP-100G-FR-S
VID                   : ES0
Date Code (yy/mm/dd) : 19/09/19
  
```

To disable the module, use the **transceiver disable** command in controller optics configuration mode:

```

Router(config)# controller optics 0/0/0/0
Router(config-Optics)# transceiver disable
Router(config-Optics)# commit
Router(config-Optics)# end
  
```

The following example shows the QSFP28 module disabled and powered down:

```
Router# show controllers optics 0/0/0/0
```

Controller State: **Down**

Transport Admin State: In Service

Laser State: Off

Optics Status

```

Optics Type: Unknown optics
Wavelength = 0.00 nm
  
```

Alarm Status:

-----

Detected Alarms: None

LOS/LOL/Fault Status:

**TX Power = N/A**

**RX Power = N/A**

Performance Monitoring: Disable

THRESHOLD VALUES

-----

Parameter	High Alarm	Low Alarm	High Warning	Low Warning
-----	-----	-----	-----	-----
Rx Power Threshold(dBm)	7.4	-10.4	4.5	-6.3
Tx Power Threshold(dBm)	7.0	-6.3	4.0	-2.4
LBC Threshold(mA)	100.00	8.00	83.00	10.00
Temp. Threshold(celsius)	75.00	-5.00	70.00	0.00
Voltage Threshold(volt)	3.63	2.97	3.46	3.13

Polarization parameters not supported by optics

Temperature = 0.00 Celsius

Voltage = 0.00 V

Transceiver Vendor Details

To re-enable the module, use the **no transceiver disable** command in controller optics configuration mode.

# Diagnostic Parameters for Optical Transceivers

*Table 48: Feature History Table*

Feature Name	Release Information	Description
Diagnostic Parameters for Optical Transceivers	Release 7.5.5	

Feature Name	Release Information	Description
		<p>You can analyze the diagnostic parameters for optical transceivers installed on a network device and detect potential issues with the optical transceivers, such as excessive power levels, abnormal temperature readings, or degradation of the optical signal. Such analysis is possible because the <b>show controllers optics</b> command now displays the following diagnostic parameters:</p> <ul style="list-style-type: none"> <li>• Effective Signal to Noise Ratio (eSNR)</li> <li>• Pulse Amplitude Modulation with Four Levels (PAM4) Level Transition Parameter (LTP)</li> <li>• Pre-Forward Error Correction (FEC) and Post-FEC Bit Error Rate (BER)</li> <li>• Frame Error Count (FERC)</li> <li>• Laser age</li> <li>• Thermoelectric Cooler (TEC) current</li> <li>• Laser frequency</li> <li>• Laser temperature</li> </ul> <p>For additional information on VDM (Versatile Diagnostics Monitoring), see the <a href="#">Common Management Interface Specification</a>.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b></p> <ul style="list-style-type: none"> <li>• The <b>observable-info</b> keyword is added to the <a href="#">show controller optics</a> command.</li> </ul> <p><b>YANG Data Model:</b></p> <ul style="list-style-type: none"> <li>• New XPath for <code>Cisco-IOS-XR-controller-optics-oper.yang</code></li> </ul>

Feature Name	Release Information	Description
		(see <a href="#">GitHub</a> , <a href="#">YANG Data Models Navigator</a> )

In order to monitor and report the performance of an optical transceiver and thereby enhancing the troubleshooting capabilities of the optical transceiver, the **observable-info** keyword is added to the **show controllers optics** command to display the diagnostics parameters. These parameters help in monitoring the health of the network when the optical transceiver heats up, when the link is down, when alarms are raised, or when there's traffic loss in the network. This improvement in the **show controllers optics** command now displays the following diagnostic parameters:

- Effective Signal to Noise Ratio (eSNR)
- Pulse Amplitude Modulation with Four Levels (PAM4) Level Transition Parameter (LTP)
- Pre-Forward Error Correction (FEC) and Post-FEC Bit Error Rate (BER)
- Frame Error Count (FERC)
- Laser age
- Thermoelectric Cooler (TEC) current
- Laser frequency
- Laser temperature



**Note** Not all optical transceivers support the **observable-info** keyword. Also, the parameters that are displayed depend on what the optical transceiver supports, that is, not all optical transceivers display the same parameters. For additional information on VDM (Versatile Diagnostics Monitoring), see the [Common Management Interface Specification](#).

### Verification

The following **show controllers optics observable-info** command displays the monitoring parameters of the optical transceiver present in the 0/0/0/9 location ID. The 0/0/0/9 location ID represents rack/slot/instance/port. Based on the requirement, the network administrators can use the displayed values of this command for monitoring and troubleshooting.

```
Router#show controllers optics 0/0/0/9 observable-info
Observable Information

[eSNR Media Input]
Unit: dB
Id      Value      TCALWarn      LowThreshWarn      HighThreshWarn      LowThreshAlarm
HighThreshAlarm      TCALWarn      Low High      Low High
Lane0    21.30      Low High      0.00      0.00      0.00
0.00      n n      n n
Lane1    22.05      0.00      0.00      0.00
0.00      n n      n n
Lane2    22.62      0.00      0.00      0.00
0.00      n n      n n
Lane3    22.05      0.00      0.00      0.00
```

```

0.00          n  n    n  n

[PAM4 Level Transition Parameter Media Input]
Unit: dB
Id      Value          LowThreshWarn    HighThresWarn    LowThreshAlarm
HighThreshAlarm    TCAWarn    TCAAlarm

          Low High    Low High
Lane0    47.79          0.00            0.00            0.00
0.00          n  n    n  n
Lane1    54.70          0.00            0.00            0.00
0.00          n  n    n  n
Lane2    64.34          0.00            0.00            0.00
0.00          n  n    n  n
Lane3    59.64          0.00            0.00            0.00
0.00          n  n    n  n

[Pre-FEC BER Minimum Media Input]
Unit: n/a
Id      Value          LowThreshWarn    HighThresWarn    LowThreshAlarm
HighThreshAlarm    TCAWarn    TCAAlarm

          Low High    Low High
Module  0.000E+00      0.000E+00      0.000E+00      0.000E+00
0.000E+00    n  n    n  n

[Pre-FEC BER Minimum Host Input]
Unit: n/a
Id      Value          LowThreshWarn    HighThresWarn    LowThreshAlarm
HighThreshAlarm    TCAWarn    TCAAlarm

          Low High    Low High
Module  0.000E+00      0.000E+00      0.000E+00      0.000E+00
0.000E+00    n  n    n  n

[Pre-FEC BER Maximum Media Input]
Unit: n/a
Id      Value          LowThreshWarn    HighThresWarn    LowThreshAlarm
HighThreshAlarm    TCAWarn    TCAAlarm

          Low High    Low High
Module  0.000E+00      0.000E+00      0.000E+00      0.000E+00
0.000E+00    n  n    n  n

[Pre-FEC BER Maximum Host Input]
Unit: n/a
Id      Value          LowThreshWarn    HighThresWarn    LowThreshAlarm
HighThreshAlarm    TCAWarn    TCAAlarm

          Low High    Low High
Module  0.000E+00      0.000E+00      0.000E+00      0.000E+00
0.000E+00    n  n    n  n

[Pre-FEC BER Average Media Input]
Unit: n/a
Id      Value          LowThreshWarn    HighThresWarn    LowThreshAlarm
HighThreshAlarm    TCAWarn    TCAAlarm

          Low High    Low High
Module  0.000E+00      0.000E+00      0.000E+00      0.000E+00
0.000E+00    n  n    n  n

[Pre-FEC BER Average Host Input]
Unit: n/a

```



Id	Value		LowThreshWarn	HighThresWarn	LowThreshAlarm
HighThreshAlarm		TCAWarn	TCAAlarm		
		Low High	Low High		
Module	0.000E+00		0.000E+00	0.000E+00	0.000E+00
0.000E+00		n n	n n		
[Pre-FEC BER Current Media Input]					
Unit: n/a					
Id	Value		LowThreshWarn	HighThresWarn	LowThreshAlarm
HighThreshAlarm		TCAWarn	TCAAlarm		
		Low High	Low High		
Module	0.000E+00		0.000E+00	0.000E+00	0.000E+00
0.000E+00		n n	n n		
[Pre-FEC BER Current Host Input]					
Unit: n/a					
Id	Value		LowThreshWarn	HighThresWarn	LowThreshAlarm
HighThreshAlarm		TCAWarn	TCAAlarm		
		Low High	Low High		
Module	0.000E+00		0.000E+00	0.000E+00	0.000E+00
0.000E+00		n n	n n		
[FERC Minimum Media Input]					
Unit: n/a					
Id	Value		LowThreshWarn	HighThresWarn	LowThreshAlarm
HighThreshAlarm		TCAWarn	TCAAlarm		
		Low High	Low High		
Module	0.000E+00		0.000E+00	0.000E+00	0.000E+00
0.000E+00		n n	n n		
[FERC Minimum Host Input]					
Unit: n/a					
Id	Value		LowThreshWarn	HighThresWarn	LowThreshAlarm
HighThreshAlarm		TCAWarn	TCAAlarm		
		Low High	Low High		
Module	0.000E+00		0.000E+00	0.000E+00	0.000E+00
0.000E+00		n n	n n		
[FERC Maximum Media Input]					
Unit: n/a					
Id	Value		LowThreshWarn	HighThresWarn	LowThreshAlarm
HighThreshAlarm		TCAWarn	TCAAlarm		
		Low High	Low High		
Module	0.000E+00		0.000E+00	0.000E+00	0.000E+00
0.000E+00		n n	n n		
[FERC Maximum Host Input]					
Unit: n/a					
Id	Value		LowThreshWarn	HighThresWarn	LowThreshAlarm
HighThreshAlarm		TCAWarn	TCAAlarm		
		Low High	Low High		
Module	0.000E+00		0.000E+00	0.000E+00	0.000E+00
0.000E+00		n n	n n		
[FERC Average Media Input]					
Unit: n/a					
Id	Value		LowThreshWarn	HighThresWarn	LowThreshAlarm

```

HighThreshAlarm      TCAWarn  TCAAlarm

      Low High  Low High
Module  0.000E+00  0.000E+00  0.000E+00  0.000E+00
0.000E+00      n  n      n  n

[FERC Average Host Input]
Unit: n/a
Id      Value
HighThreshAlarm      TCAWarn  TCAAlarm

      Low High  Low High
Module  0.000E+00  0.000E+00  0.000E+00  0.000E+00
0.000E+00      n  n      n  n

[FERC Current Media Input]
Unit: n/a
Id      Value
HighThreshAlarm      TCAWarn  TCAAlarm

      Low High  Low High
Module  0.000E+00  0.000E+00  0.000E+00  0.000E+00
0.000E+00      n  n      n  n

[FERC Current Host Input]
Unit: n/a
Id      Value
HighThreshAlarm      TCAWarn  TCAAlarm

      Low High  Low High
Module  0.000E+00  0.000E+00  0.000E+00  0.000E+00
0.000E+00      n  n      n  n

```

# Loopback on Optical Transceivers

*Table 49: Feature History Table*

Feature Name	Release Information	Description
Loopback on Optical Transceivers	Release 7.5.5	

Feature Name	Release Information	Description
		<p>You can now easily detect link failures between the optical transceiver and an external device such as a router by creating a loopback within the transceiver itself. Enabling loopback detects the fault in the physical or network connections, such as, traffic loss or a faulty optical transceiver.</p> <p>The loopback configuration allows incoming traffic within the transceiver to be redirected back to its source. By analyzing the loopback signals received at the source, it becomes possible to detect physical connectivity failures or network issues, such as packet loss or a malfunctioning transceiver.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b></p> <p>Modified the <a href="#">controller optics</a> command by adding the following keywords:</p> <ul style="list-style-type: none"> <li>• <b>host loopback internal</b></li> <li>• <b>host loopback line</b></li> <li>• <b>loopback internal</b></li> <li>• <b>loopback line</b></li> </ul> <p>The <b>information loopback</b> keyword is added to the <a href="#">show controller optics</a> command.</p> <p><b>YANG Data Model:</b></p> <ul style="list-style-type: none"> <li>• New XPath for <code>Cisco-IOS-XR-controller-optics-cfg.yang</code></li> </ul> <p>(see <a href="#">GitHub</a>, <a href="#">YANG Data Models Navigator</a>)</p>

You can now enable loopback functionality on the optical transceivers. Loopback is the process of redirecting inbound traffic or data signals from an optical transceiver back to the module itself. Re-routing traffic to its source enables utilization of the received data for diagnostic purposes, particularly in the identification and

resolution of physical connectivity issues or network-related problems, such as traffic loss or a faulty optical transceiver.

The optical transceiver is divided into two sides, the host side, which is positioned towards the router, and the media side, which is positioned towards the wire or cable media. It is possible to enable loopback on both the host side and media side of the optical transceiver.



**Note** Loopback can be performed only when the controller state is active (UP) and in the maintenance mode.

There are four types of loopback:

- Loopback Internal or Media Side Output Loopback
- Loopback Line or Media Side Input Loopback
- Host Loopback Internal or Host Side Input Loopback
- Host Loopback Line or Host Side Output Loopback

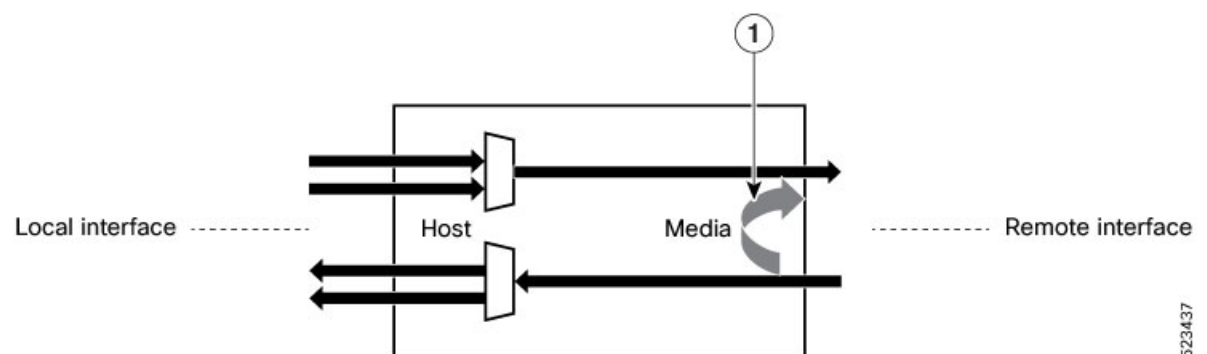


**Note** Configuring the internal loopback brings up the host interface and configuring the line loopback brings up the remote interface.

## Media Side Input Loopback Configuration

In loopback line or media side input loopback, the signals received at the media side are looped back to the media side, indicating that the received data on the media is transmitted back to the media, that is, towards the remote interface. This is indicated by the arrow labeled as 1 in the illustration.

**Figure 20: Media Side Input Loopback on the Optical Transceiver**



### Configuration Example

This example shows how to enable media side input loopback on the optical transceiver:

```
Router#config
Router(config)#controller optics 0/0/0/9
Router(config-Optics)#secondary-admin-state maintenance
Router(config-Optics)#loopback line
```

```

Loopback is a traffic-affecting operation
Router(config-Optics)#commit
Router(config-Optics)#end

```

### Running Configuration

This example shows the running configuration of the media side input loopback on the optical transceiver:

```

Router#show run controller optics 0/0/0/9
controller Optics0/0/0/9
  secondary-admin-state maintenance
  loopback line
!
```

### Verification

This example shows how to verify the media side input loopback configuration on the optical transceiver:

```

Router#show controller optics 0/0/0/9
Controller State: Up
Transport Admin State: Maintenance
Laser State: On
LED State: Green
FEC State: FEC ENABLED
Optics Status:

Optics Type: QSFPDD 400G FR4
Wavelength: 1301.00 nm
Loopback Host: None
Loopback Media: Line

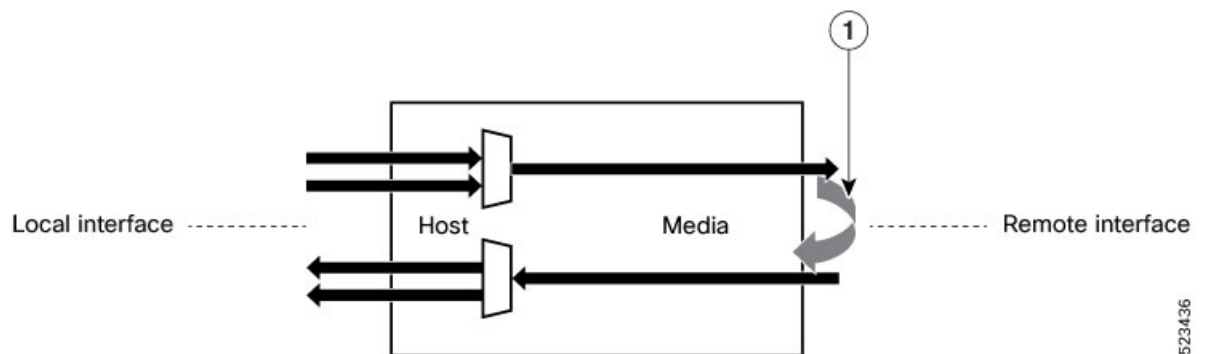
Alarm Status:
-----
Detected Alarms: None
LOS/LOL/Fault Status:
Performance Monitoring: Disable

```

## Media Side Output Loopback

In loopback internal or media side output loopback, the loopback signal originating from the NPU is looped back to the same NPU on the media or line side, towards the remote interface. This is indicated by the arrow labeled as 1 in the illustration.

**Figure 21: Media Side Output Loopback on the Optical Transceiver**



### Configuration Example

This example shows how to enable media side output loopback on the optical transceiver:

```
Router#config
Router(config)#controller optics 0/0/0/9
Router(config-Optics)#secondary-admin-state maintenance
Router(config-Optics)#loopback internal
Loopback is a traffic-affecting operation
Router(config-Optics)#commit
Router(config-Optics)#end
```

### Running Configuration

This example shows the running configuration of the media side output loopback on the optical transceiver:

```
Router#show run controller optics 0/0/0/9
controller Optics0/0/0/9
  secondary-admin-state maintenance
  loopback internal
!
```

### Verification

This example shows how to verify the media side output loopback configuration on the optical transceiver:

```
Router#show controller optics 0/0/0/9
Controller State: Up
Transport Admin State: Maintenance
Laser State: On
LED State: Green
FEC State: FEC ENABLED
Optics Status:

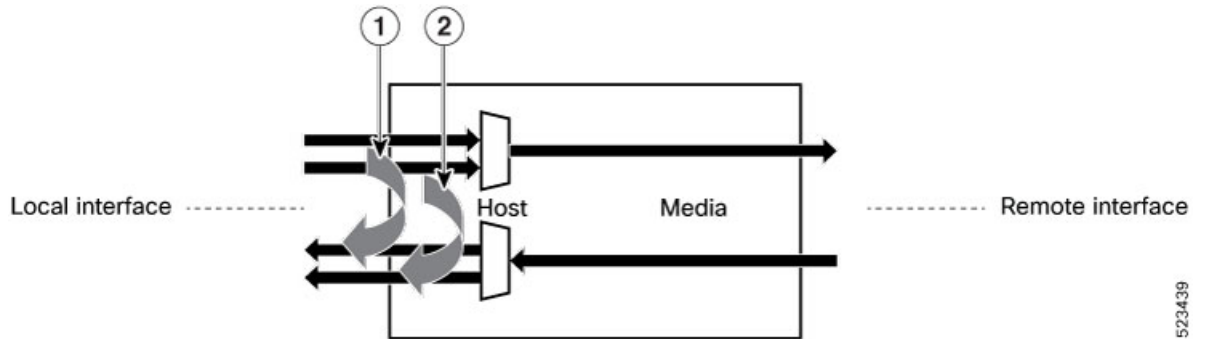
Optics Type: QSPDD 400G FR4
Wavelength: 1301.00 nm
Loopback Host: None
Loopback Media: Internal

Alarm Status:
-----
Detected Alarms: None
LOS/LOL/Fault Status:
Performance Monitoring: Disable
```

## Host Side Input Loopback Configuration

In host loopback internal or host side input loopback, the loopback signal coming from the NPU is looped back to the NPU on the host, that is, towards the local interface. This is indicated by the arrows labeled as 1 and 2 in the illustration.

Figure 22: Host Side Input Loopback on the Optical Transceiver



523439

### Configuration Example

This example shows how to enable host side input loopback on the optical transceiver:

```
Router#config
Router(config)#controller optics 0/0/0/9
Router(config-Optics)#secondary-admin-state maintenance
Router(config-Optics)#host loopback line
Loopback host is a traffic-affecting operation
Router(config-Optics)#commit
Router(config-Optics)#end
```

### Running Configuration

This example shows the running configuration of the host side input loopback on the optical transceiver:

```
Router#show run controller optics 0/0/0/9
controller Optics0/0/0/9
  secondary-admin-state maintenance
  host loopback line
!
```

### Verification

This example shows how to verify the host side input loopback configuration on the optical transceiver:

```
Router#show controller optics 0/0/0/9
Controller State: Up
Transport Admin State: Maintenance
Laser State: On
LED State: Green
FEC State: FEC ENABLED
Optics Status:

Optics Type: QSFPDD 400G FR4
Wavelength: 1301.00 nm
Loopback Host: Line
Loopback Media: None

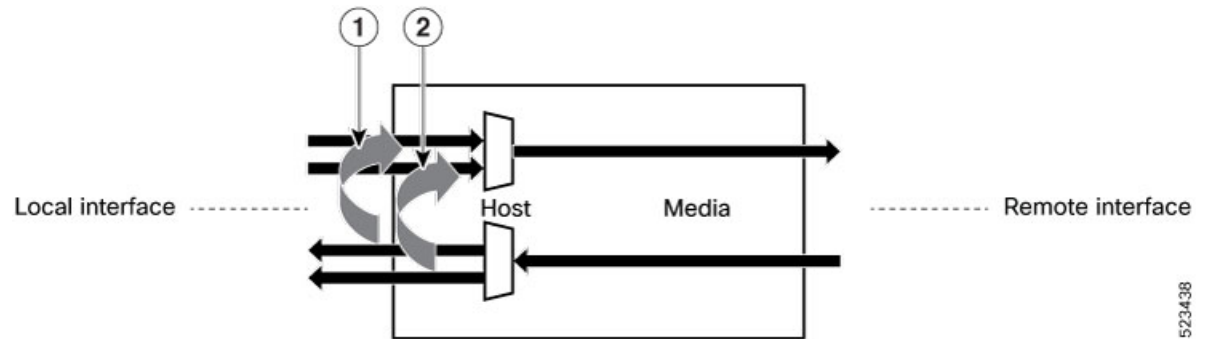
Alarm Status:
-----
Detected Alarms: None
LOS/LOL/Fault Status:
Performance Monitoring: Disable
```



# Host Side Output Loopback Configuration

In host loopback line or host side output loopback, the signals received at the host side are looped back to the host side, indicating that the received data on the host is transmitted back to the host, that is, towards the local interface. This is indicated by the arrows labeled as 1 and 2 in the illustration.

**Figure 23: Host Side Output Loopback on the Optical Transceiver**



## Configuration Example

This example shows how to enable host side output loopback on the optical transceiver:

```
Router#config
Router(config)#controller optics 0/0/0/9
Router(config-Optics)#secondary-admin-state maintenance
Router(config-Optics)#host loopback internal
Loopback host is a traffic-affecting operation
Router(config-Optics)#commit
Router(config-Optics)#end
```

## Running Configuration

This example shows the running configuration on the optical transceiver:

```
Router#show run controller optics 0/0/0/9
controller Optics0/0/0/9
  secondary-admin-state maintenance
  host loopback internal
!
```

## Verification

This example shows how to verify the host side output loopback configuration on the optical transceiver:

```
Router#show controller optics 0/0/0/9
Controller State: Up
Transport Admin State: Maintenance
Laser State: On
LED State: Green
FEC State: FEC ENABLED
Optics Status:

Optics Type: QSFPDD 400G FR4
Wavelength: 1301.00 nm
Loopback Host: Internal
Loopback Media: None

Alarm Status:
```

```
-----  
Detected Alarms: None  
LOS/LOL/Fault Status:  
Performance Monitoring: Disable
```