Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE 17

First Published: 2019-11-26

Last Modified: 2023-07-11

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

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

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

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

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

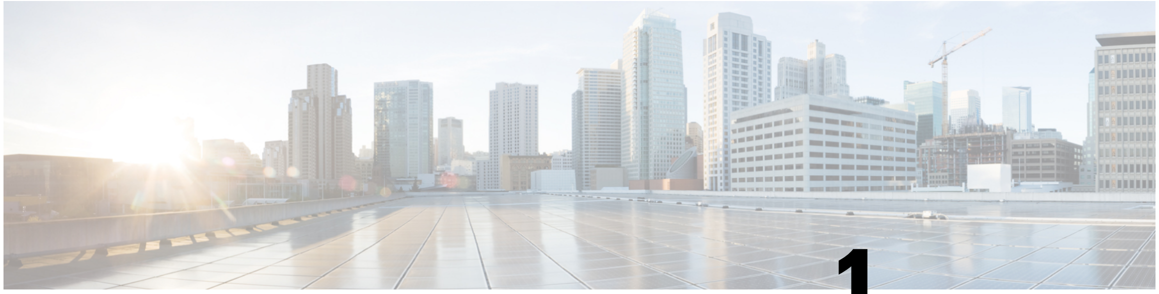
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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

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

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

CONTENTS



CHAPTER 1

Feature History

The following table lists the new and modified features supported in the Cisco NCS 4200 Series Software Configuration Guide in Cisco IOS XE 17 releases, on Cisco NCS 4201 and Cisco NCS 4202 routers.

Feature	Description
Cisco IOS XE Cupertino 17.8.1	
Increase Maximum MTU Size	Maximum Transmission Unit (MTU) is increased to a maximum of 9670 bytes on the Cisco RSP2 module. You can configure the MTU bytes using the **mtu** *bytes* command.
Cisco IOS XE Bengaluru 17.5.1	
SNMP Dying Gasp Enhancement	This feature enables FPGA based effective space utilization between Ethernet OAM and SNMP. Use the `platform-oam-snmp-dg-enable` command on Cisco router to configure this feature.
Cisco IOS XE Bengaluru 17.4.1	
CCP User Secret and Enable Secret masking	To support Common Criteria Policy validation for the masked secret.
Increase Maximum MTU Size	Maximum Transmission Unit (MTU) is increased to a maximum of 9644 bytes on the Cisco RSP3 module. You can configure the MTU bytes using the `mtu bytes` command.
VLAN Translation for RSP3	VLAN translation provides flexibility in managing VLANs and Metro Ethernet-related services. You can configure 1:1 and 2:1 VLAN translations using the sdm prefer enable_vlan_translation command on the Cisco RSP3 module.
Cisco IOS XE Amsterdam 17.1.1	
Oversubscription Support for A900-IMA8CS1Z-M NCS4200-1T16G-PS	Egress packet classification is done based on priority-based flow-control (PFC) to ensure that there are no drop in packets.

The following table lists the new and modified features supported in the Cisco NCS 4200 Series Software Configuration Guide in Cisco IOS XE 17 releases, on Cisco NCS 4206 and Cisco NCS 4216 routers.

Feature	Description
Cisco IOS XE Cupertino 17.10.1	
Enable DHCP Snooping Option 82 for RSP3	You can enable DHCP snooping option-82 on the Cisco RSP3 module using the **sdm prefer enable_dhcp_snoop** command. This feature provides additional security information to the relay agent that the information is from the trusted port.
Cisco IOS XE Cupertino 17.9.1	
Persistent Bandwidth for 8-port 10 Gigabit Ethernet Interface module (A900-IMA8Z)	This feature persistently retains the configured bandwidth value of the interface for 8-port 10 Gigabit Ethernet Interface module (A900-IMA8Z) across triggers such as interface shut or no-shut, IM reload, Stateful Switchover (SSO), and so on. This feature is only supported on Cisco RSP3 module. This feature is only supported on NCS 4206 and NCS 4216 routers.
Cisco IOS XE Cupertino 17.8.1	
Increase Maximum MTU Size	Maximum Transmission Unit (MTU) is increased to a maximum of 9670 bytes on the Cisco RSP2 module. You can configure the MTU bytes using the **mtu** *bytes* command.
Cisco IOS XE Cupertino 17.7.1	
8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module Support in Slots 1 and 2	This feature introduces the support of the 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) interface module on slots 1 and 2 and thus enables the port expansion in XFI pass through mode.

CHAPTER 2

Using Cisco IOS XE Software

Understanding Command Modes

The command modes available in the traditional Cisco IOS CLI are exactly the same as the command modes available in Cisco IOS XE.

You use the CLI to access Cisco IOS XE software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS XE software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

Table 1: Accessing and Exiting Command Modes , on page 4 describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.

Table 1: Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.
Diagnostic	The router boots up or accesses diagnostic mode in the following scenarios: • In some cases, diagnostic mode will be reached when the IOS process or processes fail. In most scenarios, however, the router will reload. • A user-configured access policy was configured using the **transport-map** command that directed the user into diagnostic mode. See the Using Cisco IOS XE Software, on page 3 chapter of this book for information on configuring access policies. • The router was accessed using a Route Switch Processor auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered and the router was configured to go into diagnostic mode when the break signal was received.	`Router(diag)#`	If the IOS process failing is the reason for entering diagnostic mode, the IOS problem must be resolved and the router rebooted to get out of diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI. If the router is accessed through the Route Switch Processor auxiliary port, access the router through another port. Accessing the router through the auxiliary port is not useful for customer purposes anyway.

Command Mode	Access Method	Prompt	Exit Method
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the **continue** command.

Universal IOS Image

Starting with XE318SP, there are two flavors of universal images supported on Cisco ASR900 series routers:

- Universal images with the "universalk9" designation in the image name: This universal image offers the strong payload cryptography Cisco IOS feature, the IPSec VPN feature.
- Universal images with the universalk9_npe" designation in the image name: The strong enforcement of encryption capabilities provided by Cisco Software Activation satisfies requirements for the export of encryption capabilities. However, some countries have import requirements that require that the platform does not support any strong crypto functionality such as payload cryptography. To satisfy the import requirements of those countries, the `npe' universal image does not support any strong payload encryption.

Starting with Cisco IOS XE Release 3.18SP, IPsec tunnel is supported only on the Cisco ASR903 and ASR907 routers with payload encryption (PE) images. IPSec requires an IPsec license to function.

Note

- IPsec license must be acquired and installed in the router for IPsec functionality to work. When you enable or disable the IPsec license, reboot is mandatory for the system to function properly. IPsec is not supported on Cisco IOS XE Everest 16.5.1.
- NPE images shipped for Cisco ASR 900 routers do not support data plane encryptions. However, control plane encryption is supported with NPE images, with processing done in software, without the crypto engine.

Understanding Diagnostic Mode

Diagnostic mode is supported.

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the RSP will simply reset when the IOS process or processes fail.
- A user-configured access policy was configured using the **transport-map** command that directs the user into diagnostic mode.
- A send break signal (**Ctrl-C** or **Ctrl-Shift-6**) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

In diagnostic mode, a subset of the commands that are also available in User EXEC mode are made available to users. Among other things, these commands can be used to:

- Inspect various states on the router, including the IOS state.
- Replace or roll back the configuration.

- Provide methods of restarting the IOS or other processes.
- Reboot hardware, such as the entire router, an RSP, an IM, or possibly other hardware components.
- Transfer files into or off of the router using remote access methods such as FTP, TFTP, SCP, and so on.

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMmon, to diagnose and troubleshoot IOS problems.

The diagnostic mode commands are stored in the non-IOS packages on the chassis, which is why the commands are available even if the IOS process is not working properly. Importantly, all the commands available in diagnostic mode are also available in privileged EXEC mode on the router even during normal router operation. The commands are entered like any other commands in the privileged EXEC command prompts when used in privileged EXEC mode.

Recommended Methods for CLI Configuration on Router

⚠

Attention Don't copy and paste the CLI configuration directly on to router console.

We recommend that you perform one of the following methods:

- Line-by-Line CLI manual configuration
- For scale configuration, use the TCL SH utility available on the router for creating configurations with appropriate delay. For more information on scripting with TCL, see Cisco IOS Scripting with TCL Configuration Guide.
- You can use the configuration file, copied to startup configuration and bring-up the router.

Accessing the CLI Using a Console

The following sections describe how to access the command-line interface (CLI) using a directly-connected console or by using Telnet or a modem to obtain a remote console:

Accessing the CLI Using a Directly Connected Console

This section describes how to connect to the console port on the router and use the console interface to access the CLI. The console port is located on the front panel of each Route Switch Processor (RSP).

Restrictions

Table 2: Feature History

Feature Name	Release	Description
CCP User Secret and Enable Secret masking	Cisco IOS XE Bengaluru 17.4.1	To support Common Criteria Policy validation for the masked secret.

- The total length of a single-line CLI must not exceed more than 256 characters as per the cli-parser component.
- Common Criteria Policy validation for masked-secret is supported for Username CLI only (a single-line command).

Connecting to the Console Port

Before you can use the console interface on the router using a terminal or PC, you must perform the following steps:

Procedure

Step 1 Configure your terminal emulation software with the following settings:

- 9600 bits per second (bps)
- 8 data bits
- No parity
- 1 stop bit
- No flow control

Step 2 Connect to the port using the RJ-45-to-RJ-45 cable and RJ-45-to-DB-25 DTE adapter or using the RJ-45-to-DB-9 DTE adapter (labeled “Terminal”).

Using the Console Interface

Every RSP has a console interface. Notably, a standby RSP can be accessed using the console port in addition to the active RSP in a dual RSP configuration.

To access the CLI using the console interface, complete the following steps:

Procedure

Step 1 After you attach the terminal hardware to the console port on the router and you configure your terminal emulation software with the proper settings, the following prompt appears:

Example:

```
Press RETURN to get started.
```

Step 2 Press **Return** to enter user EXEC mode. The following prompt appears:

Example:

```
Router>
```

Step 3 From user EXEC mode, enter the **enable** command as shown in the following example:

Example:

```
Router> enable
```

Step 4 At the password prompt, enter your system password. If an enable password has not been set on your system, this step may be skipped.The following example shows entry of the password called “enablepass”:

Example:

```
Password: enablepass
```

Step 5 When your enable password is accepted, the privileged EXEC mode prompt appears:

Example:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the console session, enter the **exit** command as shown in the following example:

Example:

```
Router# exit
```

Accessing the CLI from a Remote Console Using Telnet

This section describes how to connect to the console interface on a router using Telnet to access the CLI.

Preparing to Connect to the Router Console Using Telnet

Before you can access the router remotely using Telnet from a TCP/IP network, you need to configure the router to support virtual terminal lines (vtys) using the **line vty** global configuration command. You also should configure the vtys to require login and specify a password.

Note To prevent disabling login on the line, be careful that you specify a password with the **password** command when you configure the **login** line configuration command. If you are using authentication, authorization, and accounting (AAA), you should configure the **login authentication** line configuration command. To prevent disabling login on the line for AAA authentication when you configure a list with the **login authentication** command, you must also configure that list using the **aaa authentication login** global configuration command. For more information about AAA services, refer to the *Cisco IOS XE Security Configuration Guide,* Release 2 and *Cisco IOS Security Command Reference* publications.

In addition, before you can make a Telnet connection to the router, you must have a valid host name for the router or have an IP address configured on the router. For more information about requirements for connecting to the router using Telnet, information about customizing your Telnet services, and using Telnet key sequences, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.2SR.

Using Telnet to Access a Console Interface

To access a console interface using Telnet, complete the following steps:

Procedure

Step 1 From your terminal or PC, enter one of the following commands:

- **connect** *host* [*port*] [*keyword*]
- **telnet** *host* [*port*] [*keyword*]

In this syntax, *host* is the router hostname or an IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information, refer to the *Cisco IOS Configuration Fundamentals Command Reference* .

Note If you are using an access server, then you will need to specify a valid port number such as **telnet 172.20.52.40 2004**, in addition to the hostname or IP address.

The following example shows the **telnet** command to connect to the router named "router":

Example:

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

Step 2 At the password prompt, enter your login password. The following example shows entry of the password called "mypass":

Example:

```
User Access Verification
Password: mypass
```

Note If no password has been configured, press **Return**.

Step 3 From user EXEC mode, enter the **enable** command as shown in the following example:

Example:

```
Router> enable
```

Step 4 At the password prompt, enter your system password. The following example shows entry of the password called "enablepass":

Example:

```
Password: enablepass
```

Step 5 When the enable password is accepted, the privileged EXEC mode prompt appears:

Example:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the Telnet session, use the **exit** or **logout** command as shown in the following example:

Example:

```
Router# logout
```

Accessing the CLI from a Remote Console Using a Modem

To access the router remotely using a modem through an asynchronous connection, connect the modem to the console port.

The console port on a chassis is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is located on the front panel of the RSP.

To connect a modem to the console port, place the console port mode switch in the in position. Connect to the port using the RJ-45-to-RJ-45 cable and the RJ-45-to-DB-25 DCE adapter (labeled "Modem").

To connect to the router using the USB console port, connect to the port using a USB Type A-to-Type A cable.

Using the Auxiliary Port

The auxiliary port on the Route Switch Processor does not serve any useful purpose for customers.

This port should only be accessed under the advisement of a customer support representative.

Using Keyboard Shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

Table 3: Keyboard Shortcuts , on page 10 lists the keyboard shortcuts for entering and editing commands.

Table 3: Keyboard Shortcuts

Keystrokes	Purpose
Ctrl-B or the **Left Arrow** key[1]	Move the cursor back one character
Ctrl-F orthe **Right Arrow** key1	Move the cursor forward one character
Ctrl-A	Move the cursor to the beginning of the command line
Ctrl-E	Move the cursor to the end of the command line
Esc B	Move the cursor back one word
Esc F	Move the cursor forward one word

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Using the History Buffer to Recall Commands

The history buffer stores the last 20 commands you entered. History substitution allows you to access these commands without retyping them, by using special abbreviated commands.

Table 4: History Substitution Commands, on page 11 lists the history substitution commands.

Table 4: History Substitution Commands

Command	Purpose
Ctrl-P or the **Up Arrow** key[2]	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the **Down Arrow** key1	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the **Up Arrow** key.
`Router# show history`	While in EXEC mode, list the last several commands you have just entered.

[2] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Table 5: Help Commands and Purpose

Command	Purpose
help	Provides a brief description of the help system in any command mode.
abbreviated-command-entry **?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry <**Tab** >	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Finding Command Options Example

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS XE software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **rep** command, you would type **rep ?**.

The <cr> symbol in command help output stands for "carriage return." On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 6: Finding Command Options , on page 12 shows examples of how you can use the question mark (**?**) to assist you in entering commands.

Table 6: Finding Command Options

Command	Comment

`Router> `**`enable`**
`Password: `*`<password>`*
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a "# " from the "> "; for example, Router> to Router# .

`Router#`
`configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)# .

`Router(config)# `**`interface gigabitEthernet ?`**
`  <0-0>  GigabitEthernet interface number`
`  <0-1>  GigabitEthernet interface number`
`Router(config)#`**`interface gigabitEthernet 0?`**
`.  /  <0-0>`
`Router(config)#`**`interface gigabitEthernet 0/?`**
`  <0-5>  Port Adapter number`
`Router(config)#`**`interface gigabitEthernet 0/0?`**
`/`
`Router(config)#`**`interface gigabitEthernet 0/0/?`**
`  <0-15>  GigabitEthernet interface number`
`Router(config)#`**`interface gigabitEthernet 0/0/0?`**
`.  <0-23>`
`Router(config)#`**`interface gigabitEthernet 0/0/0`**
	Enter interface configuration mode by specifying the serial interface that you want to configure using the **interface serial** global configuration command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.
	When the <cr> symbol is displayed, you can press Enter to complete the command.
	You are in interface configuration mode when the prompt changes to Router(config-if)# .

<table>
<tr><th>Command</th><th>Comment</th></tr>
<tr><td>

```
Router(config-if)# ?
Interface configuration commands:
  .
  .
  .
  ip                  Interface Internet Protocol config
 commands
  keepalive            Enable keepalive
  lan-name             LAN Name command
  llc2                 LLC2 Interface Subcommands
  load-interval        Specify interval for load
calculation for an
                       interface
  locaddr-priority     Assign a priority group
  logging              Configure logging for interface
  loopback            Configure internal loopback on an
 interface
  mac-address         Manually set interface MAC address

  mls                 mls router sub/interface commands

  mpoa                 MPOA interface configuration
commands
  mtu                  Set the interface Maximum
Transmission Unit (MTU)
  netbios             Use a defined NETBIOS access list
 or enable
                       name-caching
  no                   Negate a command or set its
defaults
  nrzi-encoding        Enable use of NRZI encoding
  ntp                  Configure NTP
  .
  .
  .
Router(config-if)#
```

</td><td>Enter <b>?</b> to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.</td></tr>
</table>

Command	Comment
Router(config-if)# **ip ?** Interface IP configuration subcommands: access-group Specify access control for packets accounting Enable IP accounting on this interface address Set the IP address of an interface authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp DVMRP interface commands hello-interval Configures IP-EIGRP hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures IP-EIGRP hold time . . . Router(config-if)# **ip**	Enter the command that you want to configure for the interface. This example uses the **ip** command. Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Router(config-if)# **ip address ?**
  A.B.C.D   IP address
  negotiated   IP Address negotiated over PPP
Router(config-if)# **ip address**
	Enter the command that you want to configure for the interface. This example uses the **ip address** command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword.
	A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

Router(config-if)# **ip address 172.16.0.1 ?** A.B.C.D IP subnet mask Router(config-if)# **ip address 172.16.0.1**	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.
Router(config-if)# **ip address 172.16.0.1 255.255.255.0** **?** secondary Make this IP address a secondary address <cr> Router(config-if)# **ip address 172.16.0.1 255.255.255.0**	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask. Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**. A <cr> is displayed; you can press **Enter** to complete the command, or you can enter another keyword.

Command	Comment

`Router(config-if)# ip address 172.16.0.1 255.255.255.0`
`Router(config-if)#`
	In this example, **Enter** is pressed to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to re-enable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Many CLI commands also have a **default** form. By issuing the command **default** *command-name* , you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function of the **default** form of the command when the **default** form performs a different function than the plain and **no** forms of the command. To see what default commands are available on your system, enter **default ?** in the appropriate command mode.

Saving Configuration Changes

Use the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

This task saves the configuration to NVRAM.

Managing Configuration Files

On the chassis, the startup configuration file is stored in the nvram: file system and the running-configuration files are stored in the system: file system. This configuration file storage setup is not unique to the chassis and is used on several Cisco router platforms.

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router's other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.

The **copy** command can be used to backup startup configuration files. Below are some examples showing the startup configuration file in NVRAM being backed up:

Example 1: Copying Startup Configuration File to Bootflash

```
Router# dir bootflash:
Directory of bootflash:/
   11  drwx       16384   Feb 2 2000 13:33:40 +05:30  lost+found
15105  drwx        4096   Feb 2 2000 13:35:07 +05:30  .ssh
45313  drwx        4096  Nov 17 2011 17:36:12 +05:30  core
75521  drwx        4096   Feb 2 2000 13:35:11 +05:30  .prst_sync
90625  drwx        4096   Feb 2 2000 13:35:22 +05:30  .rollback_timer
105729  drwx        8192  Nov 21 2011 22:57:55 +05:30  tracelogs
30209  drwx        4096   Feb 2 2000 13:36:17 +05:30  .installer
1339412480 bytes total (1199448064 bytes free)
Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?
3517 bytes copied in 0.647 secs (5436 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/
   11  drwx       16384   Feb 2 2000 13:33:40 +05:30  lost+found
15105  drwx        4096   Feb 2 2000 13:35:07 +05:30  .ssh
45313  drwx        4096  Nov 17 2011 17:36:12 +05:30  core
75521  drwx        4096   Feb 2 2000 13:35:11 +05:30  .prst_sync
90625  drwx        4096   Feb 2 2000 13:35:22 +05:30  .rollback_timer
   12  -rw-           0   Feb 2 2000 13:36:03 +05:30  tracelogs.878
105729  drwx        8192  Nov 21 2011 23:02:13 +05:30  tracelogs
30209  drwx        4096   Feb 2 2000 13:36:17 +05:30  .installer
   13  -rw-        1888  Nov 21 2011 23:03:17 +05:30  startup-config
1339412480 bytes total (1199439872 bytes free)
```

Example 2: Copying Startup Configuration File to USB Flash Disk

```
Router# dir usb0:
Directory of usb0:/
43261  -rwx   208904396  May 27 2008 14:10:20 -07:00
ncs4200rsp3-adventerprisek9.02.01.00.122-33.XNA.bin
255497216 bytes total (40190464 bytes free)
Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?
3172 bytes copied in 0.214 secs (14822 bytes/sec)
Router# dir usb0:
Directory of usb0:/
43261  -rwx   208904396  May 27 2008 14:10:20 -07:00
ncs4200rsp3-adventerprisek9.02.01.00.122-33.XNA.bin43262 -rwx
 3172 Jul 2 2008 15:40:45 -07:00  startup-config255497216 bytes total (40186880 bytes free)
```

Example 3: Copying Startup Configuration File to a TFTP Server

```
Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_confg]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)
```

For more detailed information on managing configuration files, see the *Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S* .

Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case sensitive):

show *command* | {**append** | **begin** | **exclude** | **include** | **redirect** | **section** | **tee** | **count**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression “protocol” appears:

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is up, line protocol is up
Serial4/0/0 is up, line protocol is up
Serial4/1/0 is up, line protocol is up
Serial4/2/0 is administratively down, line protocol is down
Serial4/3/0 is administratively down, line protocol is down
```

Powering Off the Router

Before you turn off a power supply, make certain the chassis is grounded and you perform a soft shutdown on the power supply. Not performing a soft shutdown will often not harm the router, but may cause problems in certain scenarios.

To perform a soft shutdown before powering off the router, enter the **reload** command to halt the system and then wait for ROM Monitor to execute before proceeding to the next step.

The following screenshot shows an example of this process:

```
Router# reload
Proceed with reload? [confirm]
*Jun 18 19:38:21.870: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
command.
```

Place the power supply switch in the Off position after seeing this message.

Finding Support Information for Platforms and Cisco Software Images

Cisco software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or the software release notes.

Using Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Using Software Advisor

To see if a feature is supported by a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com at http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl.

You must be a registered user on Cisco.com to access this tool.

Using Software Release Notes

Cisco IOS XE software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- New feature information
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. Refer to Cisco Feature Navigator for cumulative feature information.

CHAPTER 3

Console Port Telnet and SSH Handling

This chapter covers the following topics:

Important Notes and Restrictions

- The Telnet and SSH settings made in the transport map override any other Telnet or SSH settings when the transport map is applied to the Management Ethernet interface.
- Only local usernames and passwords can be used to authenticate users entering a Management Ethernet interface. AAA authentication is not available for users accessing the router through a Management Ethernet interface using persistent Telnet or persistent SSH.
- Applying a transport map to a Management Ethernet interface with active Telnet or SSH sessions can disconnect the active sessions. Removing a transport map from an interface, however, does not disconnect any active Telnet or SSH sessions.
- Configuring the diagnostic and wait banners i s optional but recommended. The banners are especially useful as indicators to users of the status of their Telnet or SSH attempts.

Console Port Overview

The console port on the chassis is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is used to access the chassis and is located on the front panel of the Route Switch Processor (RSP).

For information on accessing the chassis using the console port, see the "Accessing the CLI Using a Console" section on page 1-4 .

Connecting Console Cables

For information about connecting console cables to the chassis, see the NCS 4200 Hardware Installation Guides.

Installing USB Device Drivers

For instructions on how to install device drivers in order to use the USB console port, see the NCS 4200 Hardware Installation Guides.

Console Port Handling Overview

Users using the console port to access the chassis are automatically directed to the IOS command-line interface, by default.

If a user is trying to access the router through the console port and sends a break signal (a break signal can be sent by entering **Ctrl-C** or **Ctrl-Shift-6**, or by entering the **send break** command at the Telnet prompt) before connecting to the IOS command-line interface, the user is directed into diagnostic mode by default if the non-RPIOS sub-packages can be accessed.

These settings can be changed by configuring a transport map for the console port and applying that transport map to the console interface.

Telnet and SSH Overview

Telnet and Secure Shell (SSH) can be configured and handled like Telnet and SSH on other Cisco platforms. For information on traditional Telnet, see the **line** command in the Cisco IOS Terminal Services Command Reference guide.

For information on configuring traditional SSH, see the Secure Shell Configuration Guide, Cisco IOS XE Release 3S.

The chassis also supports persistent Telnet and persistent SSH. Persistent Telnet and persistent SSH allow network administrators to more clearly define the treatment of incoming traffic when users access the router through the Management Ethernet port using Telnet or SSH. Notably, persistent Telnet and persistent SSH provide more robust network access by allowing the router to be configured to be accessible through the Ethernet Management port using Telnet or SSH even when the IOS process has failed.

Persistent Telnet and Persistent SSH Overview

In traditional Cisco routers, accessing the router using Telnet or SSH is not possible in the event of an IOS failure. When Cisco IOS fails on a traditional Cisco router, the only method of accessing the router is through the console port. Similarly, if all active IOS processes have failed on a chassis that is not using persistent Telnet or persistent SSH, the only method of accessing the router is through the console port.

With persistent Telnet and persistent SSH, however, users can configure a transport map that defines the treatment of incoming Telnet or SSH traffic on the Management Ethernet interface. Among the many configuration options, a transport map can be configured to direct all traffic to the IOS command-line interface, diagnostic mode, or to wait for an IOS vty line to become available and then direct users into diagnostic mode when the user sends a break signal while waiting for the IOS vty line to become available. If a user uses Telnet or SSH to access diagnostic mode, that Telnet or SSH connection will be usable even in scenarios when no IOS process is active. Therefore, persistent Telnet and persistent SSH introduce the ability to access the router via diagnostic mode when the IOS process is not active. For information on diagnostic mode, see the “Understanding Diagnostic Mode” section on page 1-3 .

For more information on the various other options that are configurable using persistent Telnet or persistent SSH transport map see the Configuring Persistent Telnet, on page 23 and the Configuring Persistent SSH, on page 25 .

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type console transport-map-name** **Example:** `Router(config)# transport-map type console consolehandler`	Creates and names a transport map for handling console connections, and enter transport map configuration mode.
Step 4	**connection wait** [**allow interruptible** | **none**] **Example:** `Router(config-tmap)# connection wait none` **Example:**	Specifies how a console connection will be handled using this transport map: • **allow interruptible**—The console connection waits for an IOS vty line to become available, and also allows user to enter diagnostic mode by interrupting a console connection waiting for the IOS vty

	Command or Action	Purpose
		line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The console connection immediately enters diagnostic mode.

Step 5	**banner** [**diagnostic** | **wait**] *banner-message*
	Example:
	`Router(config-tmap)# banner diagnostic X`
	Example:
	`Enter TEXT message.  End with the character 'X'.`
	Example:
	`--Welcome to Diagnostic Mode--`
	Example:
	`X`
	Example:
	`Router(config-tmap)#`
	Example:
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS vty line as a result of the console transport map configuration.
		• **diagnostic**—Creates a banner message seen by users directed into diagnostic mode as a result of the console transport map configuration.
		• **wait**—Creates a banner message seen by users waiting for the IOS vty to become available.
		• *banner-message*—The banner message, which begins and ends with the same delimiting character.

Step 6	**exit** **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	**transport type console** *console-line-number* **input** *transport-map-name* **Example:** `Router(config)# transport type console 0 input consolehandler`	Applies the settings defined in the transport map to the console interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** comm and.

Examples

In the following example, a transport map to set console port access policies is created and attached to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
Welcome to diagnostic mode
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

Configuring Persistent Telnet

Before you begin

For a persistent Telnet connection to access an IOS vty line on the chassis, local login authentication must be configured for the vty line (the **login** command in line configuration mode). If local login authentication is not configured, users will not be able to access IOS using a Telnet connection into the Management Ethernet interface with an applied transport map. Diagnostic mode will still be accessible in this scenario.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type persistent telnet** *transport-map-name* **Example:** `Router(config)# transport-map type persistent telnet telnethandler`	Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** {**interruptible**}| **none** {**disconnect**}] **Example:** `Router(config-tmap)# connection wait none` **Example:**	Specifies how a persistent Telnet connection will be handled using this transport map: • **allow**—The Telnet connection waits for an IOS vty line to become available, and exits the router if interrupted. • **allow interruptible**—The Telnet connection waits for the IOS vty line to

	Command or Action	Purpose
		become available, and also allows user to enter diagnostic mode by interrupting a Telnet connection waiting for the IOS vty line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The Telnet connection immediately enters diagnostic mode. • **none disconnect**—The Telnet connection does not wait for the IOS vty line and does not enter diagnostic mode, so all Telnet connections are rejected if no vty line is immediately available in IOS.

Step 5	**banner** [**diagnostic** | **wait**] *banner-message*
	Example:
	`Router(config-tmap)# banner diagnostic X`
	Example:
	`Enter TEXT message.  End with the character 'X'.`
	Example:
	`--Welcome to Diagnostic Mode--`
	Example:
	`X`
	Example:
	`Router(config-tmap)#`
	Example:
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS vty line as a result of the persistent Telnet configuration.
		• **diagnostic**—creates a banner message seen by users directed into diagnostic mode as a result of the persistent Telnet configuration.
		• **wait**—creates a banner message seen by users waiting for the vty line to become available.
		• *banner-message*—the banner message, which begins and ends with the same delimiting character.

Step 6	**transport interface type** *num* **Example:** `Router(config-tmap)# transport interface gigabitethernet 0`	Applies the transport map settings to the Management Ethernet interface (interface gigabitethernet 0). Persistent Telnet can only be applied to the Management Ethernet interface on the chassis. This step must be taken before applying the transport map to the Management Ethernet interface.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 8	**transport type persistent telnet input** *transport-map-name* **Example:** `Router(config)# transport type persistent telnet input telnethandler`	Applies the settings defined in the transport map to the Management Ethernet interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type persistent telnet** comm and.

Examples

In the following example, a transport map that will make all Telnet connections wait for an IOS vty line to become available before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)#
connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

Configuring Persistent SSH

This task describes how to configure persistent SSH.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type persistent ssh** *transport-map-name* **Example:** `Router(config)# transport-map type persistent ssh sshhandler`	Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** {**interruptible**}| **none** {**disconnect**}] **Example:** `Router(config-tmap)# connection wait allow interruptible` **Example:**	Specifies how a persistent SSH connection will be handled using this transport map: • **allow**—The SSH connection waits for the vty line to become available, and exits the router if interrupted. • **allow interruptible**—The SSH connection waits for the vty line to become available, and also allows users to enter diagnostic mode by interrupting a SSH connection waiting for the vty line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The SSH connection immediately enters diagnostic mode. • **none disconnect**—The SSH connection does not wait for the vty line from IOS and does not enter diagnostic mode, so all SSH connections are rejected if no vty line is immediately available.
Step 5	**rsa keypair-name** *rsa-keypair-name* **Example:** `Router(config-tmap)# rsa keypair-name sshkeys`	Names the RSA keypair to be used for persistent SSH connections. For persistent SSH connections, the RSA keypair name must be defined using this command in transport map configuration mode. The RSA keypair definitions defined elsewhere on the router, such as through the use of the **ip ssh rsa keypair-name** command, do not apply to persistent SSH connections.

	Command or Action	Purpose
		No *rsa-keypair-name* is defined by default.
Step 6	**authentication-retries***number-of-retries* **Example:** `Router(config-tmap)# authentication-retries 4`	(Optional) Specifies the number of authentication retries before dropping the connection. The default *number-of-retries* is 3.

Step 7	**banner** [**diagnostic** | **wait**] *banner-message*
	Example:
	`Router(config-tmap)# banner diagnostic X`
	Example:
	`Enter TEXT message.  End with the character 'X'.`
	Example:
	`--Welcome to Diagnostic Mode--`
	Example:
	`X`
	Example:
	`Router(config-tmap)#`
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the vty line as a result of the persistent SSH configuration.
		• **diagnostic**—Creates a banner message seen by users directed into diagnostic mode as a result of the persistent SSH configuration.
		• **wait**—Creates a banner message seen by users waiting for the vty line to become active.
		• *banner-message*—The banner message, which begins and ends with the same delimiting character.

Step 8	**time-out***timeout-interval* **Example:** `Router(config-tmap)# time-out 30`	(Optional) Specifies the SSH time-out interval in seconds. The default *timeout-interval* is 120 seconds.
Step 9	**transport interface type** *num* **Example:** `Router(config-tmap)# transport interface gigabitethernet 0`	Applies the transport map settings to the Management Ethernet interface (interface gigabitethernet 0). Persistent SSH can only be applied to the Management Ethernet interface on the chassis.
Step 10	**exit** **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 11	**transport type persistent ssh input** *transport-map-name* **Example:**	Applies the settings defined in the transport map to the Management Ethernet interface. The *transport-map-name* for this command must match the *transport-map-name* defined

	Command or Action	Purpose
	`Router(config)# transport type persistent ssh input sshhandler`	in the **transport-map type persistent ssh** command .

Examples

In the following example, a transport map that will make all SSH connections wait for the vty line to become active before connecting to the router is configured and applied to the Management Ethernet interface (interface gigabitethernet 0). The RSA keypair is named sshkeys.

This example only uses the commands required to configure persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
```

In the following example, a transport map is configured that will apply the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH will wait for the vty line to become active, but will enter diagnostic mode if the attempt to access IOS through the vty line is interrupted.
- The RSA keypair name is “sshkeys”
- The connection allows one authentication retry.
- The banner “--Welcome to Diagnostic Mode--” will appear if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner “--Waiting for vty line--” will appear if the connection is waiting for the vty line to become active.

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1


Router(config-tmap)# banner diagnostic X


Enter TEXT message.  End with the character 'X'.


--Welcome to Diagnostic Mode--


X


Router(config-tmap)#banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for vty line--
X
Router(config-tmap)#
time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
```

Viewing Console Port, SSH, and Telnet Handling Configurations

Use the **show transport-map all name** *transport-map-name* | **type console persistent ssh telnet**]]] EXEC or privileged EXEC command to view the transport map configurations.

In the following example, a console port, persistent SSH, and persistent Telnet transport are configured on the router and various forms of the **show transport-map** command are entered to illustrate the various ways the **show transport-map** command can be entered to gather transport map configuration information.

```
Router# show transport-map all
Transport Map:
  Name: consolehandler
  Type: Console Transport
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for the IOS CLI
  bshell banner:
Welcome to Diagnostic Mode
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS prompt
  Bshell banner:

Welcome to Diagnostic Mode
SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys
Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS process
  Bshell banner:
Welcome to Diagnostic Mode
Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport
Connection:
  Wait option: Wait Allow
Router# show transport-map type console
Transport Map:
  Name: consolehandler
  Type: Console Transport
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for the IOS CLI
  Bshell banner:
Welcome to Diagnostic Mode
Router# show transport-map type persistent ssh
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS prompt
  Bshell banner:
Welcome to Diagnostic Mode
SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys
Router# show transport-map type persistent telnet

Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS process
  Bshell banner:
Welcome to Diagnostic Mode
Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport
Connection:
  Wait option: Wait Allow
Router# show transport-map name telnethandler
Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS process
  Bshell banner:
Welcome to Diagnostic Mode
Router# show transport-map name consolehandler
Transport Map:
  Name: consolehandler
  Type: Console Transport
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for the IOS CLI
  Bshell banner:
Welcome to Diagnostic Mode
Router# show transport-map name sshhandler
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport
```

```
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS prompt
  Bshell banner:
Welcome to Diagnostic Mode
SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys
Router#
```

The **show platform software configuration access policy** command can be used to view the current configurations for the handling of incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection, as well as any information on the currently configured banners. Unlike **show transport-map**, this command is available in diagnostic mode so it can be entered in cases when you need transport map configuration information but cannot access the IOS CLI.

```
Router# show platform software configuration access policy
The current access-policies
Method      : telnet
Rule        : wait
Shell banner:
Wait banner :
Method      : ssh
Rule        : wait
Shell banner:
Wait banner :
Method      : console
Rule        : wait with interrupt
Shell banner:
Wait banner :
```

In the following example, the connection policy and banners are set for a persistent SSH transport map, and the transport map is enabled.

The **show platform software configuration access policy** output is given both before the new transport map is enabled and after the transport map is enabled so the changes to the SSH configuration are illustrated in the output.

```
Router# show platform software configuration access policy

The current access-policies
Method      : telnet
Rule        : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode
Wait banner :
Waiting for IOS Process
Method      : ssh
Rule        : wait
Shell banner:
Wait banner :
Method      : console
Rule        : wait with interrupt
Shell banner:
Wait banner :
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
Router(config)# exit
Router# show platform software configuration access policy
The current access-policies
Method      : telnet
Rule        : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode
Wait banner :
Waiting for IOS process
Method      : ssh
Rule        : wait with interrupt
Shell banner:
Welcome to Diag Mode
Wait banner :
Waiting for IOS
Method      : console
Rule        : wait with interrupt
Shell banner:
Wait banner :
```

CHAPTER 4

Using the Management Ethernet Interface

This chapter covers the following topics:

Gigabit Ethernet Management Interface Overview

The chassis has one Gigabit Ethernet Management Ethernet interface on each Route Switch Processor.

The purpose of this interface is to allow users to perform management tasks on the router; it is basically an interface that should not and often cannot forward network traffic but can otherwise access the router, often via Telnet and SSH, and perform most management tasks on the router. The interface is most useful before a router has begun routing, or in troubleshooting scenarios when the interfaces are inactive.

The following aspects of the Management Ethernet interface should be noted:

- Each RSP has a Management Ethernet interface, but only the active RSP has an accessible Management Ethernet interface (the standby RSP can be accessed using the console port, however).
- IPv4, IPv6, and ARP are the only routed protocols supported for the interface.
- The interface provides a method of access to the router even if the interfaces or the IOS processes are down.
- The Management Ethernet interface is part of its own VRF. For more information, see the Gigabit Ethernet Management Interface VRF, on page 34.

Gigabit Ethernet Port Numbering

The Gigabit Ethernet Management port is always GigabitEthernet0.

In a dual RSP configuration, the Management Ethernet interface on the active RSP will always be Gigabit Ethernet 0, while the Management Ethernet interface on the standby RSP will not be accessible using the Cisco IOS CLI in the same telnet session. The standby RSP can be accessed via console port using telnet.

The port can be accessed in configuration mode like any other port on the chassis.

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitethernet0
Router(config-if)#
```

IP Address Handling in ROMmon and the Management Ethernet Port

IP addresses can be configured using ROMmon (**IP_ADDRESS=** and **IP_SUBNET_MASK=** commands) and the IOS command-line interface (the **ip address** command in interface configuration mode).

Assuming the IOS process has not begun running on the chassis, the IP address that was set in ROMmon acts as the IP address of the Management Ethernet interface. In cases where the IOS process is running and has taken control of the Management Ethernet interface, the IP address specified when configuring the Gigabit Ethernet 0 interface in the IOS CLI becomes the IP address of the Management Ethernet interface. The ROMmon-defined IP address is only used as the interface address when the IOS process is inactive.

For this reason, the IP addresses specified in ROMmon and in the IOS CLI can be identical and the Management Ethernet interface will function properly in single RSP configurations.

In dual RSP configurations, however, users should never configure the IP address in the ROMmon on either RP0 or RP1 to match each other or the IP address as defined by the IOS CLI. Configuring matching IP addresses introduces the possibility for an active and standby Management Ethernet interface having the same IP address with different MAC addresses, which will lead to unpredictable traffic treatment or possibility of an RSP boot failure.

Gigabit Ethernet Management Interface VRF

The Gigabit Ethernet Management interface is automatically part of its own VRF. This VRF, which is named "Mgmt-intf," is automatically configured on the chassis and is dedicated to the Management Ethernet interface; no other interfaces can join this VRF. Therefore, this VRF does not participate in the MPLS VPN VRF or any other network-wide VRF.

Placing the management ethernet interface in its own VRF has the following effects on the Management Ethernet interface:

- Many features must be configured or used inside the VRF, so the CLI may be different for certain Management Ethernet functions on the chassis than on Management Ethernet interfaces on other routers.
- Prevents transit traffic from traversing the router. Because all of the interfaces and the Management Ethernet interface are automatically in different VRFs, no transit traffic can enter the Management Ethernet interface and leave an interface, or vice versa.
- Improved security of the interface. Because the Mgmt-intf VRF has its own routing table as a result of being in its own VRF, routes can only be added to the routing table of the Management Ethernet interface if explicitly entered by a user.

The Management Ethernet interface VRF supports both IPv4 and IPv6 address families.

Common Ethernet Management Tasks

Because users can perform most tasks on a router through the Management Ethernet interface, many tasks can be done by accessing the router through the Management Ethernet interface.

This section documents common configurations on the Management Ethernet interface and includes the following sections:

Viewing the VRF Configuration

The VRF configuration for the Management Ethernet interface is viewable using the **show running-config vrf** command.

This example shows the default VRF configuration:

```
Router# show running-config vrf
Building configuration...
Current configuration : 351 bytes
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
(some output removed for brevity)
```

Viewing Detailed VRF Information for the Management Ethernet VRF

To see detailed information about the Management Ethernet VRF, enter the **show vrf detail Mgmt-intf** command.

```
Router# show vrf detail Mgmt-intf
VRF Mgmt-intf (VRF Id = 4085); default RD <not set>; default VPNID <not set>
  Interfaces:
    Gi0
Address family ipv4 (Table ID = 4085 (0xFF5)):
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 (Table ID = 503316481 (0x1E000001)):
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

Setting a Default Route in the Management Ethernet Interface VRF

To set a default route in the Management Ethernet Interface VRF, enter the following command

ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 *next-hop-IP-address*

Setting the Management Ethernet IP Address

The IP address of the Management Ethernet port is set like the IP address on any other interface.

Below are two simple examples of configuring an IPv4 address and an IPv6 address on the Management Ethernet interface.

IPv4 Example

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ip address A.B.C.D A.B.C.D
```

IPv6 Example

```
Router(config)# interface GigabitEthernet 0
```

Router(config-if)# **ipv6 address** *X:X:X:X::X*

Telnetting over the Management Ethernet Interface

Telnetting can be done through the VRF using the Management Ethernet interface.

In the following example, the router telnets to 172.17.1.1 through the Management Ethernet interface VRF:

```
Router# telnet 172.17.1.1 /vrf Mgmt-intf
```

Pinging over the Management Ethernet Interface

Pinging other interfaces using the Management Ethernet interface is done through the VRF.

In the following example, the router pings the interface with the IP address of 172.17.1.1 through the Management Ethernet interface.

```
Router# ping vrf Mgmt-intf 172.17.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Copy Using TFTP or FTP

To copy a file using TFTP through the Management Ethernet interface, the **ip tftp source-interface GigabitEthernet 0** command must be entered before entering the **copy tftp** command because the **copy tftp** command has no option of specifying a VRF name.

Similarly, to copy a file using FTP through the Management Ethernet interface, the **ip ftp source-interface GigabitEthernet 0** command must be entered before entering the **copy ftp** command because the **copy ftp** command has no option of specifying a VRF name.

TFTP Example

```
Router(config)# ip tftp source-interface gigabitethernet 0
```

FTP Example

```
Router(config)# ip ftp source-interface gigabitethernet 0
```

NTP Server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server over the Management Ethernet interface, enter the **ntp server vrf Mgmt-intf** command and specify the IP address of the device providing the update.

The following CLI provides an example of this procedure.

```
Router(config)# ntp server vrf Mgmt-intf 172.17.1.1
```

SYSLOG Server

To specify the Management Ethernet interface as the source IPv4 or IPv6 address for logging purposes, enter the **logging host** *ip-address* **vrf Mgmt-intf** command.

The following CLI provides an example of this procedure.

```
Router(config)# logging host <ip-address> vrf Mgmt-intf
```

SNMP-related services

To specify the Management Ethernet interface as the source of all SNMP trap messages, enter the **snmp-server source-interface traps gigabitEthernet 0** command.

The following CLI provides an example of this procedure:

```
Router(config)# snmp-server source-interface traps gigabitEthernet 0
```

Domain Name Assignment

The IP domain name assignment for the Management Ethernet interface is done through the VRF.

To define the default domain name as the Management Ethernet VRF interface, enter the **ip domain-name vrf Mgmt-intf** *domain* command.

```
Router(config)# ip domain-name vrf Mgmt-intf cisco.com
```

DNS service

To specify the Management Ethernet interface VRF as a name server, enter the **ip name-server vrf Mgmt-intf** *IPv4-or-IPv6-address* command.

```
Router(config)# ip name-server vrf Mgmt-intf
 IPv4-or-IPv6-address
```

RADIUS or TACACS+ Server

To group the Management VRF as part of a AAA server group, enter the **ip vrf forward Mgmt-intf** command when configuring the AAA server group.

The same concept is true for configuring a TACACS+ server group. To group the Management VRF as part of a TACACS+ server group, enter the **ip vrf forwarding Mgmt-intf** command when configuring the TACACS+ server group.

Radius Server Group Configuration

```
Router(config)# aaa group server radius hello
Router(config-sg-radius)# ip vrf forwarding Mgmt-intf
```

Tacacs+ Server Group Example

```
outer(config)# aaa group server tacacs+ hello
Router(config-sg-tacacs+)# ip vrf forwarding Mgmt-intf
```

VTY lines with ACL

To ensure an access control list (ACL) is attached to vty lines that are and are not using VRF, use the **vrf-also** option when attaching the ACL to the vty lines.

```
Router(config)# line vty 0 4
Router(config-line)# access-class 90 in vrf-also
```

CHAPTER 5

Configuring Ethernet Interfaces

This chapter provides information about configuring the Gigabit Ethernet interface modules.

For more information about the commands used in this chapter, see the Cisco IOS XE 3S Command References.

Configuring Ethernet Interfaces

This section describes how to configure the Gigabit and Ten Gigabit Ethernet interface modules and includes information about verifying the configuration.

Limitations and Restrictions

- Conflicting VLAN ranges and the exact VLAN values on different EFPs for same interface is not supported. When the EFP of an interface has second-dot1q between the range from 1000 to 2000, then any no other service instance can have a second-dot1q within the same range.
- VRF-Aware Software Infrastructure (VASI) interface commnads **interface vasileft** and interface vasiright are not supported .
- Interface modules have slot restrictions, see NCS 4200 Hardware Installation Guides.
- MPLS MTU is *not* supported.
- On the RSP3 module, MTU value configured for a BDI interface should match with the MTU configuration for all the physical interfaces, which have a service instance associated with this BDI.
- If the packet size is more than the configured MTU value and exceeds 1Mbps, packets are dropped. Packets are fragmented when the packet size is more than the configured MTU value and when traffic is lesser than 1Mbps.
- To replace the configured interface module with a different interface module in a particular slot, run the **hw-module subslot *slot-num* default** command.
- Giant counters are not supported.

- Ingress counters are not incremented for packets of the below packet format on the RSP3 module for the 10 Gigabit Ethernet interfaces, 100 Gigabit Ethernet interfaces, and 40 Gigabit Ethernet interfaces:

  MAC header---->Vlan header---->Length/Type

  When these packets are received on the RSP3 module, the packets are not dropped, but the counters are not incremented.

- If the IM is shutdown using **hw-module subslot shutdown** command, then the IM goes out-of-service. You should perform a Stateful Switchover (SSO) in the interim, as the IM needs to be re-inserted for successful reactivation.

- Following are some of the IMs that are not supported on certain slots when IPsec license is enabled:
  - The below IMs are not supported on the Slot 11 on the Cisco ASR 907 router:
    - SPA_TYPE_ETHER_IM_8x10GE
    - SPA_TYPE_ETHER_IM_2x40GE
  - The below IMs are not supported on the Slot 2 on the Cisco ASR 903 router for RSP3-200 and RSP3-400:
    - SPA_TYPE_ETHER_IM_8xGE_SFP_1x10GE
    - SPA_TYPE_ETHER_IM_8xGE_CU_1x10GE
    - SPA_TYPE_ETHER_IM_1x10GE
    - SPA_TYPE_ETHER_IM_8x10GE
    - SPA_TYPE_OCX_IM_OC3OC12
    - SPA_TYPE_ETHER_IM_8xGE_SFP
    - SPA_TYPE_ETHER_IM_8xGE_CU

- CTS signal goes down, when control signal frequency is configured more than 5000 ms and timeout setting is more than 20,000 ms (4x control_frequency), which is greater than the OIR time (~20s) for a selected subordinate to complete an OIR cycle. This results in the primary being unaware that the subordinate is down and CTS of all subordinates are down too. To avoid this situation, ensure that the timeout is shorter than the OIR time of the subordinate. Set the control frequency to less than or equal to 5000 ms and the timeout setting to less than or equal to 20,000 ms before you perform OIR.

- You may ignore the following error that is seen during IM OIR or while the router goes down:

  ```
  %IOSXE-2-PLATFORM: R1/0: kernel: Address caused MCE = 0x0, DEAR = <>
  ```

- Interfaces with CU SFP flap twice during router boot up or IM OIR.

- In routers with Cu optics, physical SFP OIR, the following I2C error occurs:

  ```
  %IOMD_IMFPGA-3-I2C_WRITE: C0/1: iomd: IM slot 1: An I2C write has
  failed for addr: 0x56 reg: 0x16 data: 0x0
  ```

  As physical SFP OIR is an externally triggered event, it is not possible to prevent such errors. To avoid the error, we recommend to put the port in Shutdown state and do OIR.

Configuring an Interface

This section lists the required configuration steps to configure Gigabit and Ten Gigabit Ethernet interface modules.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 2	Do one of the following:
	• **interface gigabitethernet** *slot/subslot/port*
	• **interface tengigabitethernet** *slot/subslot/port*
	Example:
	`Router(config)# interface gigabitethernet 0/0/1`
	Example:
	Example:
	`Router(config)# interface tengigabitethernet 0/0/1`
		Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where:
		Note The slot number is always 0.

Step 3	**ip address** *ip-address mask* {**secondary**} | **dhcp** {**client-id** *interface-name*}{**hostname** *host-name*}] **Example:** `Router(config-if)# ip address 192.168.1.1 255.255.255.255 dhcp hostname host1`	Sets a primary or secondary IP address for an interface that is using IPv4, where: • *ip-address* —The IP address for the interface. • *mask* —The mask for the associated IP subnet. • **secondary**—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. • **dhcp**—Specifies that IP addresses will be assigned dynamically using DHCP. • **client-id** *interface-name*—Specifies the client identifier. The *interface-name* sets the client identifier to the hexadecimal MAC address of the named interface.

	Command or Action	Purpose
		- **hostname** *host-name*—Specifies the hostname for the DHCP purposes. The *host-name* is the name of the host to be placed in the DHCP option 12 field.
Step 4	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	(Optional) Disables automatic negotitation. **Note** Use the **speed** command only when the mode is set to no negotiation auto.

Step 5	**speed**{ **10** | **100** | **1000**}
	Example:
	`Router(config-if)# speed 1000`
		(Optional) Specifies the speed for an interface to transmit at 10, 100, and 1000 Mbps (1 Gbps), where the default is 1000 Mbps.

Step 6	**mtu** *bytes* **Example:** `Router(config-if)# mtu 1500`	(As Required) Specifies the maximum packet size for an interface, where: - *bytes*—The maximum number of bytes for a packet. The default is 1500 bytes; the range is from 1500 to 9216. Effective Cisco IOS XE release 17.4.1, 9644 MTU bytes are supported on the Cisco RSP3 module.
Step 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 250 ip 192.168.10.1`	Creates or enables the Hot Standby Router Protocol (HSRP) group using its number and virtual IP address, where: - (Optional) *group-number*—The group number on the interface for which HSRP is being enabled. The range is from 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. - (Optional on all but one interface if configuring HSRP) *ip-address*—The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. - (Optional) **secondary**—Specifies that the IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary

	Command or Action	Purpose
		IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router. **Note** This command is required only for configurations that use HSRP. **Note** This command enables HSRP but does not configure it further.
Step 8	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.

Specifying the Interface Address on an Interface Module

To configure or monitor Ethernet interfaces, you need to specify the physical location of the interface module and interface in the CLI. The interface address format is slot/subslot/port, where:

- slot—The chassis slot number in the chassis where the interface module is installed.

Note The interface module slot number is always 0.

- subslot—The subslot where the interface module is installed. Interface module subslots are numbered from 0 to 5 for ASR 903 and from 0 to 15 for ASR 907, from bottom to top.
- port—The number of the individual interface port on an interface module.

The following example shows how to specify the first interface (0) on an interface module installed in the first interface module slot:

```
Router(config)# interface GigabitEthernet 0/0/0
 no ip address
 shutdown
 negotiation auto
 no cdp enable
```

Configuring Hot Standby Router Protocol

Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts without relying on the availability of any single router. You can deploy HSRP in a group of routers to select an active router and a standby router. (An *active* router is the router of choice for routing packets; a *standby* router is a router that takes over the routing duties when an active router fails, or when preset conditions are met).

HSRP is enabled on an interface by entering the **standby** [*group-number*] **ip** [*ip-address* [**secondary**]] command. The **standby** command is also used to configure various HSRP elements. This document does not discuss more complex HSRP configurations. For additional information on configuring HSRP, see to the

HSRP section of the Cisco IP Configuration Guide publication that corresponds to your Cisco IOS XE software release. In the following HSRP configuration, standby group 2 on Gigabit Ethernet port 0/1/0 is configured at a priority of 110 and is also configured to have a preemptive delay should a switchover to this port occur:

```
Router(config)#interface GigabitEthernet 0/1/0
Router(config-if)#standby 2 ip 192.168.1.200
Router(config-if)#standby 2 priority 110
Router(config-if)#standby 2 preempt
```

The maximum number of different HSRP groups that can be created on one physical interface is 4. If additional groups are required, create 4 groups on the physical interface, and the remaining groups on the BDI or on another physical interface.

Note TCAM space utilization changes when HSRP groups are configured on the router. If HSRP groups are configured the TCAM space is utilized. Each HSRP group takes 1 TCAM entry. The “Out of TCAM” message may be displayed if total number of TCAM space used by HSRP groups and prefixes on the router exceeds scale limit.

Note HSRP state flaps with sub-second “Hello” or “Dead” timers.

Restrictions

HSRPv2 is not supported.

Verifying HSRP

To verify the HSRP information, use the show standby command in EXEC mode:

```
Router# show standby
Ethernet0 - Group 0
Local state is Active, priority 100, may preempt
Hellotime 3 holdtime 10
Next hello sent in 0:00:00
Hot standby IP address is 198.92.72.29 configured
Active router is local
Standby router is 198.92.72.21 expires in 0:00:07
Standby virtual mac address is 0000.0c07.ac00
Tracking interface states for 2 interfaces, 2 up:
UpSerial0
UpSerial1
```

Modifying the Interface MTU Size

Table 7: Feature History

Feature Name	Release	Description
Increase Maximum MTU Size	Cisco IOS XE Bengaluru 17.4.1	Maximum Transmission Unit (MTU) is increased to a maximum of 9644 bytes on the Cisco RSP3 module. You can configure the MTU bytes using the **mtu** *bytes* command.
Increase Maximum MTU Size	Cisco IOS XE Cupertino 17.8.1	Maximum Transmission Unit (MTU) is increased to a maximum of 9670 bytes on the Cisco RSP2 module. You can configure the MTU bytes using the **mtu** *bytes* command.

Note The maximum number of unique MTU values that can be configured on the physical interfaces on the chassis is 8. Use the **show platform hardware pp active interface mtu command** to check the number of values currently configured on the router. This is not applicable on Cisco ASR 900 RSP3 Module.

The Cisco IOS software supports three different types of configurable maximum transmission unit (MTU) options at different levels of the protocol stack:

- Interface MTU—The interface module checks the MTU value of incoming traffic. Different interface types support different interface MTU sizes and defaults. The interface MTU defines the maximum packet size allowable (in bytes) for an interface before drops occur. If the frame is smaller than the interface MTU size, but is not smaller than the minimum frame size for the interface type (such as 64 bytes for Ethernet), then the frame continues to process.
- MPLS MTU—If the MPLS MTU is set to a value, for example, 1500 bytes, the value is programmed as 1504 bytes at the hardware level to allow the addition of one label. Consider the case of pseudowire. If the packet size of Layer 2 traffic sent with four bytes of Frame Check Sequence (FCS) to the pseudowire is 1500 bytes, then and four bytes of pseudowire control word and one pseudowire label (label size is four bytes) is added to the packet, the packet size is now 1508 bytes with FCS. However, note that while calculating the packet size, FCS is not considered. So the calculated packet size is 1504 bytes, which is equal to the MPLS MTU programmed in the hardware. This packet is forwarded as expected.

  However, if another label is added to this packet, the packet size becomes 1508 bytes without FCS. This value is greater than programmed MTU value, so this packet is dropped. This restriction applies not only to pseudowire, but to the entire MPLS network.

  To ensure that packets are not dropped, MPLS MTUs should be set considering the maximum size of the label stack that is added to the packet in the network.

For the Gigabit Ethernet interface module on the chassis, the default MTU size is 1500 bytes. The interface module automatically adds an additional 22 bytes to the configured MTU size to accommodate some of the additional overhead.

Increase Maximum MTU Size on RSP3 module

Effective Cisco IOS XE Bengaluru 17.4.1, a maximum of 9644 MTU bytes are supported on the Cisco RSP3 module.

Prior to Cisco IOS XE Bengaluru 17.4.1, you can configure a maximum of 9216 bytes on the Cisco RSP3 module.

Increase Maximum MTU Size on RSP2 module

Effective Cisco IOS XE Cupertino 17.8.1, a maximum of 9644 MTU bytes are supported on the Cisco RSP2 module.

Prior to this release, you can configure a maximum of 9216 bytes on the Cisco RSP2 module.

Limitations

- In EtherLike-MIB, the **dot3StatsFrameTooLongs** frames count in SNMP increases when the frame packet size is more than the default MTU.
- If the packet size is more than the configured MTU value and exceeds 1Mbps, packets are dropped. Packets are fragmented when the packet size is more than the configured MTU value and when traffic is lesser than 1Mbps.
- Due to hardware limitation on the Cisco RSP2 module, ping is not supported with MTU size of greater than 9215 bytes.

Interface MTU Configuration Guidelines

When configuring the interface MTU size, we recommend you consider the following guidelines:

Note The default interface MTU size always accommodates a 1500-byte packet, plus 22 additional bytes to cover the following additional overhead.

- An interface (without tagging applied), sends a maximum of 1522 bytes of data. Here the interface sends 1508 (Data) bytes + 14 (Layer 2 header) bytes = 1522 bytes.
- An interface (with tagging applied) sends bytes as follows:
  - **dot1q tagging** — Interface sends 1504 (Data) bytes + 14 (Layer 2 header) + 4 (dot1q encapsulation header) bytes = 1522 bytes.
  - **double dot1q tagging** — Interface sends 1500 (Data) bytes + 14 (Layer 2 header) + 8 (double dot1q encapsulation header) bytes = 1522 bytes.
- Interface MTU is not supported on BDI Interface.
- If you are using MPLS labels, then you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Note If you are using MPLS, ensure that the **mpls mtu** command is configured for a value less than or equal to the interface MTU. This is not applicable on the RSP3 Module.

Configuring Interface MTU

To modify the MTU size on an interface, use the following command in interface configuration mode:

Command	Purpose
mtu *bytes* `Router(config-if)# mtu bytes`	Configures the maximum packet size for an interface, where: • *bytes*— Specifies the maximum number of bytes for a packet. The default is 1500 bytes and the maximum configurable MTU is 9216 bytes.

To return to the default MTU size, use the **no** form of the command.

Note When IP FRR over BDI is configured, the maximum allowed packet size is 1504 bytes.

When the BGP-PIC core is enabled, a packet destined to a prefix that is learnt through eBGP, is dropped if the packet size is greater than 1504 bytes. To work around this limitation, do one of the following:

- Disable the BGP-PIC core,
- Use the static route, or
- Use routed-port instead of BDI.

Verifying the MTU Size

To verify the MTU size for an interface, use the **show interfaces gigabitethernet** privileged EXEC command and observe the value shown in the “MTU” field.

The following example shows an MTU size of 1500 bytes for interface port 0 (the second port) on the Gigabit Ethernet interface module installed in slot 1:

```
Router# show interfaces gigabitethernet 0/1/0
GigabitEthernet0/1/0 is up, line protocol is up
  Hardware is  NCS4200-1T8LR-PS, address is d0c2.8216.0590 (bia d0c2.8216.0590)
  MTU 1500 bytes
, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 22/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

Configuring the Encapsulation Type

The only encapsulation supported by the interface modules is IEEE 802.1Q encapsulation for virtual LANs (VLANs).

Note VLANs are only supported on Ethernet Virtual Connection (EVC) service instances and Trunk Ethernet Flow Point (EFP) interfaces.

Configuring Autonegotiation on an Interface

Gigabit Ethernet interfaces use a connection-setup algorithm called *autonegotiation.* Autonegotiation allows the local and remote devices to configure compatible settings for communication over the link. Using autonegotiation, each device advertises its transmission capabilities and then agrees upon the settings to be used for the link.

For the Gigabit Ethernet interfaces on the chassis, flow control is autonegotiated when autonegotiation is enabled. Autonegotiation is enabled by default.

When enabling autonegotiation, consider these guidelines:

- If autonegotiation is disabled on one end of a link, it must be disabled on the other end of the link. If one end of a link has autonegotiation disabled while the other end of the link does not, the link will not come up properly on both ends.
- Flow control is enabled by default.
- Flow control will be on if autonegotiation is disabled on both ends of the link.

Enabling Autonegotiation

To enable autonegotiation on a Gigabit Ethernet interface, use the following command in interface configuration mode:

Command	Purpose
negotiation auto `Router(config-if)# negotiation auto`	Enables autonegotiation on a Gigabit Ethernet interface. Advertisement of flow control occurs.

Disabling Autonegotiation

Autonegotiation is automatically enabled and can be disabled on Gigabit Ethernet interfaces . During autonegotiation, advertisement for flow control, speed, and duplex occurs, depending on the media (fiber or copper) in use.

Speed and duplex configurations can be advertised using autonegotiation. The values that are negotiated are:

- For Gigabit Ethernet interfaces using RJ-45 ports and for Copper (Cu) SFP ports—10, 100, and 1000 Mbps for speed and full-duplex mode. Link speed is not negotiated when using fiber interfaces.

To disable autonegotiation, use the following command in interface configuration mode:

Command	Purpose
no negotiation auto `Router(config-if)# no negotiation auto`	Disables autonegotiation on Gigabit Ethernet interfaces. No advertisement of flow control occurs.

Configuring Carrier Ethernet Features

For information about configuring an Ethernet interface as a layer 2 Ethernet virtual circuit (EVC) or Ethernet flow point (EFP), see the Ethernet Virtual Connections.

Saving the Configuration

To save your running configuration to NVRAM, use the following command in privileged EXEC configuration mode:

Command	Purpose
copy running-config startup-config `Router# copy running-config startup-config`	Writes the new configuration to NVRAM.

For information about managing your system image and configuration files, refer to the Cisco IOS Configuration Fundamentals Configuration Guide and publications that correspond to your Cisco IOS software release.

Shutting Down and Restarting an Interface

You can shut down and restart any of the interface ports on an interface module independently of each other. Shutting down an interface stops traffic and enters the interface into an "administratively down" state.

If you are preparing for an OIR of an interface module, it is not necessary to independently shut down each of the interfaces prior to deactivation of the module.

Command	Purpose

shutdown
`router#configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`router(config)`
`router(config)#interface GigabitEthernet 0/1/0`
`router(config-if)#shutdown`
no shutdown
`router#configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`router(config)`
`router(config)#interface GigabitEthernet 0/1/0`
`router(config-if)#no shutdown`
	Restarts, stops, or starts an interface.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display the configuration settings, you can use the **show interfaces gigabitethernet** command to get detailed information on a per-port basis for your Gigabit Ethernet interface module.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the Gigabit Ethernet interface module, use the **show interfaces gigabitethernet** command.

The following example provides sample output for interface port 0 on the interface module located in slot 1:

```
Router# show interfaces GigabitEthernet0/1/0
GigabitEthernet0/1/0 is up, line protocol is up
  Hardware is  NCS4200-1T8LR-PS, address is d0c2.8216.0590 (bia d0c2.8216.0590)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 08:59:45, output hang never
  Last clearing of show interface counters 09:00:18
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     11 packets input, 704 bytes, 0 no buffer
     Received 11 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

Verifying Interface Module Status

You can use various **show** commands to view information specific to SFP, XFP, CWDM, and DWDM optical transceiver modules.

Note The **show interface transceiver** command is *not* supported on the router.

To check or verify the status of an SFP Module or XFP Module, use the following **show** commands:

Use **show hw-module** *slot/subslot* **transceiver** *port* **status** or **show interfaces** *interface* **transceiver detail** to view the threshold values for temperature, voltage and so on.

For example, **show hw-module subslot 0/5 transceiver 1 status** or **show interfaces tenGigabitEthernet 0/5/1 transceiver detail** .

Command	Purpose
show hw-module *slot/subslot* **transceiver** *port* **idprom**	Displays information for the transceiver identification programmable read only memory (idprom). **Note** Transceiver types must match for a connection between two interfaces to become active.
show hw-module *slot/subslot* **transceiver** *port* **idprom status**	Displays information for the transceiver initialization status. **Note** The transmit and receive optical power displayed by this command is useful for troubleshooting Digital Optical Monitoring (DOM). For interfaces to become active, optical power must be within required thresholds.
show hw-module *slot/subslot* **transceiver** *port* **idprom dump**	Displays a dump of all EEPROM content stored in the transceiver.

The following **show hw-module subslot** command sample output is for 1000BASE BX10-U:

```
Router#show hw-module subslot 0/2 transceiver 0 idprom brief

IDPROM for transceiver GigabitEthernet0/2/0:
  Description                               = SFP or SFP+ optics (type 3)
  Transceiver Type:                         = 1000BASE BX10-U (259)
  Product Identifier (PID)                  = GLC-BX-U
  Vendor Revision                           = 1.0
  Serial Number (SN)                        = NPH20441771
  Vendor Name                               = CISCO-NEO
  Vendor OUI (IEEE company ID)              = 00.15.06 (5382)
  CLEI code                                 = IPUIAG5RAC
  Cisco part number                         = 10-2094-03
```

```
 Device State                              = Enabled.
  Date code (yy/mm/dd)                      = 16/11/12
  Connector type                            = LC.
  Encoding                                  = 8B10B (1)
  Nominal bitrate                           = GE (1300 Mbits/s)
  Minimum bit rate as % of nominal bit rate = not specified
  Maximum bit rate as % of nominal bit rate = not specified
Router#
```

The following **show hw-module subslot** command sample output is for an SFP+ 10GBASE-SR:

```
Router#show hw-module subslot 0/2 transceiver 8 idprom brief

IDPROM for transceiver TenGigabitEthernet0/2/8:
  Description                               = SFP or SFP+ optics (type 3)
  Transceiver Type:                         = SFP+ 10GBASE-SR (273)
  Product Identifier (PID)                  = SFP-10G-SR
  Vendor Revision                           = 2
  Serial Number (SN)                        = JUR2052G19W
  Vendor Name                               = CISCO-LUMENTUM
  Vendor OUI (IEEE company ID)              = 00.01.9C (412)
  CLEI code                                 = COUIA8NCAA
  Cisco part number                         = 10-2415-03
  Device State                              = Enabled.
  Date code (yy/mm/dd)                      = 16/12/21
  Connector type                            = LC.
  Encoding                                  = 64B/66B (6)
  Nominal bitrate                           =  (10300 Mbits/s)
  Minimum bit rate as % of nominal bit rate = not specified
  Maximum bit rate as % of nominal bit rate = not specified
Router#
```

Note VID for optics displayed in **show inventory** command and vendor revision shown in **idprom detail** command output are stored in diffrent places in Idprom.

Configuring LAN/WAN-PHY Controllers

The LAN/WAN-PHY controllers are configured in the physical layer control element of the Cisco IOS XE software.

Restrictions for LAN/WAN-PHY Mode

- Effective with Cisco IOS XE Release 3.18.1SP, A900-IMA8Z Interface Modules (IM) support LAN/WAN-PHY mode.
- The following A900-IMA8Z IM alarms are not supported:
  - NEWPTR
  - PSE
  - NSE
  - FELCDP

- FEAISP

Configuring LAN-PHY Mode

This section describes how to configure LAN-PHY mode on the Gigabit Ethernet interface modules.

Procedure

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td><b>Step 1</b></td><td><b>show controllers wanphy</b> <i>slot/subslot/port</i>
<b>Example:</b>
<pre>
Router# show controllers wanphy 0/1/0

TenGigabitEthernet0/1/0
<b>Mode of Operation: WAN Mode</b>
SECTION
LOF = 0   LOS   = 0
                   BIP(B1) = 0
LINE
AIS = 0   RDI   = 0
 FEBE = 0   BIP(B2) = 0
PATH
AIS = 0   RDI   = 0
 FEBE = 0   BIP(B3) = 0
LOP = 0   NEWPTR = 0
 PSE = 0   NSE   = 0
WIS ALARMS
SER   = 0   FELCDP = 0
 FEAISP = 0
WLOS   = 0   PLCD   = 0
LFEBIP = 0   PBEC   = 0
Active Alarms[All defects]: SWLOF LAIS
PAIS SER
Active Alarms[Highest Alarms]: SWLOF
Alarm reporting enabled for: SF SWLOF
B1-TCA B2-TCA PLOP WLOS
Rx(K1/K2): 00/00 Tx(K1/K2): 00/00
S1S0 = 00, C2 = 0x1A
PATH TRACE BUFFER: UNSTABLE
Remote J1 Byte :
BER thresholds: SD = 10e-6 SF = 10e-3
TCA thresholds: B1 = 10e-6 B2 = 10e-6
  B3 = 10e-6
</pre></td><td>Displays the configuration mode of the LAN/WAN-PHY controller. Default configuration mode is LAN.
If the configuration mode is WAN, complete the rest of the procedure to change the configuration mode to LAN.
• <i>slot</i> /<i>subslot</i> /<i>port</i>—The location of the interface.</td></tr>
<tr><td><b>Step 2</b></td><td><b>configure terminal</b>
<b>Example:</b>
<pre>
Router# configure terminal
</pre></td><td>Enters global configuration mode.</td></tr>
<tr><td><b>Step 3</b></td><td>Do the following:
• <b>hw-module subslot</b> <i>slot/subslot</i> <b>interface</b> <i>port</i> <b>enable LAN</b>
<b>Example:</b></td><td>Configures LAN-PHY mode for the Ethernet interface module.
• <i>slot</i> /<i>subslot</i> /<i>port</i>—The location of the interface.</td></tr>
</table>

	Command or Action	Purpose

	`Router(config)# hw-module subslot 0/1 enable LAN`
	Example:
	`Router(config)# hw-module subslot 0/1 interface 1 enable LAN`
		Use the **hw-module subslot** *slot/subslot* **interface** *port enable LAN* command to configure the LAN-PHY mode for the Ethernet interface module.

Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Step 5	**show controllers wanphy** *slot/subslot/port*
	Example:
	`Router# show controllers wanphy 0/1/2`
	`TenGigabitEthernet0/1/2`
	`Mode of Operation: LAN Mode`
		Displays configuration mode for the LAN/WAN-PHY controller. The example shows the mode of operation as LAN mode for the Cisco 8-Port 10 Gigabit Ethernet LAN/WAN-PHY Controller.

Configuring WAN-PHY Mode

This section describes how to configure WAN-PHY mode on the Gigabit Ethernet interface modules.

Procedure

	Command or Action	Purpose

Step 1	**show controllers wanphy** *slot/subslot/port*
	Example:
	`Router# show controllers wanphy 0/1/0`
	`TenGigabitEthernet0/1/0`
	`Mode of Operation: LAN Mode`
		Displays the configuration mode of the WAN-PHY controller. Default configuration mode is LAN.
		• *slot* /*subslot* /*port*—The location of the interface.

Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Do the following: • **hw-module subslot** *slot/subslot***interface** *port enable WAN* **Example:** `Router(config)# hw-module subslot 0/1 enable WAN` **Example:**	Configures WAN-PHY mode for the Ethernet interface module. • *slot* /*subslot* /*port* —The location of the interface. Use the **hw-module subslot** *slot/subslot* **interface** *port enable WAN* command to configure the WAN-PHY mode for the Ethernet interface module.

	Command or Action	Purpose

	`Router(config)# hw-module subslot 0/1`
	`interface 1 enable WAN`	

Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Step 5	**show controllers wanphy** *slot/subslot/port*
	Example:
	`Router# show controllers wanphy 0/1/5`
	`TenGigabitEthernet0/1/5`
	`Mode of Operation: WAN Mode`
	`SECTION`
	`  LOF = 0             LOS    = 0`
	`                     BIP(B1) = 0`
	`LINE`
	`  AIS = 0             RDI    = 0`
	`   FEBE = 0          BIP(B2) = 0`
	`PATH`
	`  AIS = 0             RDI    = 0`
	`   FEBE = 0          BIP(B3) = 0`
	`  LOP = 0             NEWPTR = 0`
	`   PSE  = 0          NSE     = 0`
	`WIS ALARMS`
	`  SER    = 0          FELCDP = 0`
	`   FEAISP = 0`
	`  WLOS   = 0          PLCD   = 0`
	`  LFEBIP = 0          PBEC   = 0`
	`Active Alarms[All defects]: SWLOF LAIS`
	`PAIS SER`
	`Active Alarms[Highest Alarms]: SWLOF`
	`Alarm reporting enabled for: SF SWLOF`
	`B1-TCA B2-TCA PLOP WLOS`
	`  Rx(K1/K2): 00/00  Tx(K1/K2): 00/00`
	`  S1S0 = 00, C2 = 0x1A`
	`PATH TRACE BUFFER: UNSTABLE`
	`Remote J1 Byte :`
	`BER thresholds:  SD = 10e-6  SF = 10e-3`
	`TCA thresholds:  B1 = 10e-6  B2 = 10e-6`
	`  B3 = 10e-6`
		Displays configuration mode for the LAN/WAN-PHY controller. The example shows the mode of operation as WAN mode for the Cisco 8-Port 10 Gigabit Ethernet LAN/WAN-PHY Controller.

Configuring WAN-PHY Error Thresholds

This section describes how to configure WAN-PHY Signal Failure (SF) and Signal Degrade (SD) Bit Error Rate (BER) reporting and thresholds.

An SF alarm is triggered if the line bit error (B2) rate exceeds a user-provisioned threshold range (over the range of 10e-3 to 10e-9).

An SD alarm is declared if the line bit error (B2) rate exceeds a user-provisioned threshold range (over the range of 10e-3 to 10e-9). If the B2 errors cross the SD threshold, a warning about link quality degradation is triggered. The WAN-PHY alarms are useful for some users who are upgrading their Layer 2 core network from a SONET ring to a 10-Gigabit Ethernet ring.

Before you begin

The controller must be in the WAN-PHY mode before configuring the SF and SD BER reporting and thresholds.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**controller wanphy** *slot/subslot/port* **Example:** `Router(config)# controller wanphy 0/3/0`	Enters WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN-PHY controller. *slot* /*subslot* /*port* —The location of the interface.

Step 3	**wanphy** {**delay** | **flag** | **report-alarm** | **threshold** {**b1-tca** | **b2-tca** | **sd-ber** | **sf-ber** [*bit error rate*]}}
	Example:
	`Router(config-controller)# wanphy threshold b1-tca 6`
		Configures WAN-PHY controller processing.
		• delay—Delays WAN-PHY alarm triggers.
		• flag—Specifies byte values.
		• report-alarm—Configures WAN-PHY alarm reporting.
		• threshold—Sets BER threshold values.
		  • b1-tca—Sets B1 alarm BER threshold.
		  • b2-tca—Sets B2 alarm BER threshold.
		  • sd-ber—Sets Signal Degrade BER threshold.
		  • sf-ber—Sets Signal Fail BER threshold.
		• bit error rate— Specifies bit error rate.

Step 4	**end**
	Example:
	`Router(config-controller)# end`
		Exits controller configuration mode and enters privileged EXEC mode.

Configuration Examples

Example: Basic Interface Configuration

The following example shows how to enter the global configuration mode to configure an interface, configure an IP address for the interface, and save the configuration:

```
! Enter global configuration mode.

!

Router# configure terminal

! Enter configuration commands, one per line. End with CNTL/Z.

!

! Specify the interface address.

!

Router(config)# interface gigabitethernet 0/0/1

!

! Configure an IP address.

!

Router(config-if)# ip address 192.168.50.1 255.255.255.0

!

! Start the interface.

!

Router(config-if)# no shut

!

! Save the configuration to NVRAM.

!

Router(config-if)# exit
```

```
Router# copy running-config startup-config
```

Example: MTU Configuration

Note The maximum number of unique MTU values that can be configured on the physical interfaces on the chassis is eight. Use the **show platform hardware pp active interface mtu command** to check the number of values currently configured on the router.

The following example shows how to set the MTU interface to 9216 bytes.

Note The interface module automatically adds an additional 38 bytes to the configured MTU interface size.

```
! Enter global configuration mode.

!

Router# configure terminal

! Enter configuration commands, one per line. End with CNTL/Z.

!

! Specify the interface address

!

Router(config)# interface gigabitethernet 0/0/1

!

! Configure the interface MTU.

!

Router(config-if)# mtu 9216
```

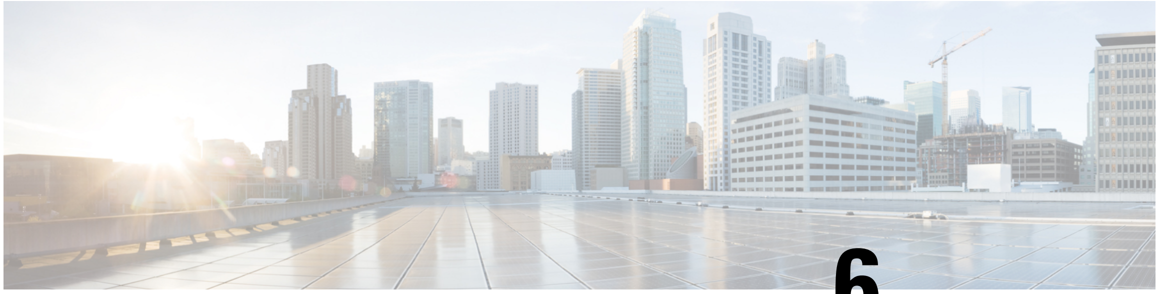
Example: VLAN Encapsulation

The following example shows how to configure interface module port 2 (the third port) and configure the first interface on the VLAN with the ID number 268 using IEEE 802.1Q encapsulation:

```
! Enter global configuration mode.
```

```
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Enter configuration commands, one per line. End with CNTL/Z.
!
Router(config)# service instance 10 ethernet
!
! Configure dot1q encapsulation and specify the VLAN ID.
Router(config-subif)# encapsulation dot1q 268
!
```

Note VLANs are supported only on EVC service instances and Trunk EFP interfaces.



CHAPTER 6

Configuring T1/E1 Interfaces

This chapter provides information about configuring the T1/E1 interface module on the chassis. It includes the following sections:

For information about managing your system images and configuration files, refer to the Cisco IOS Configuration Fundamentals Configuration Guide and publications.

For more information about the commands used in this chapter, refer to the Cisco IOS Command Reference publication for your Cisco IOS software release.

Configuration Tasks

This section describes how to configure the following T1/E1 interface modules for the chassis.

Table 8: Supported T1/E1 Interface Module

T1/E1 Interface Module	Part Number
16-port T1/E1 Interface Module	A900-IMA16D
8-portT1/E1 Interface Module	A900-IMA8D
32-Port T1/E1 Interface Module	A900-IMA32D

This section includes the following topics:

Limitations

This section describes the software limitations that apply when configuring the T1/E1 interface module.

- The following interface modules are not supported on the RSP3 module:
  - 16-port T1/E1 interface module
  - 8-portT1/E1 interface module

  - 32-portT1/E1 interface module

- The **configure replace** command is not supported on the T1/E1 interface modules.
- The chassis does *not* support more than 16 IMA groups on each T1/E1 interface module.
- The chassis only supports the following BERT patterns: 2^11, 2^15, 2^20-O153, and 2^20-QRSS.
- L2TPv3 encapsulation is not supported.
- Replacing a configured interface module with a different interface module in the same slot is not supported.
- Mixed configurations of features are not supported on the same port.
- The Payload calculation per unit for T1/E1 interface module is:
  - Framed E1 / T1 with no. of time Slots less than 4 –> Payload = 4 x no. of time slots.
  - Framed E1 / T1 with no. of Time Slots greater than or equal 4 -> Payload = 2 x no. of time slots.
  - Unframed T1, C11 –> Payload = 48 (2 x 24 (all slots)).
  - Unframed E1, C12 –> Payload = 64 (2 x32(all slots))
- Channelization is not supported for serial interfaces. However, channelization is supported for CEM at the DS0 level.

Required Configuration Tasks

This section lists the required configuration steps to configure the T1/E1 interface module. Some of the required configuration commands implement default values that might be appropriate for your network. If the default value is correct for your network, then you do not need to configure the command.

Setting the Card Type

The interface module is not functional until the card type is set. Information about the interface module is not indicated in the output of any show commands until the card type has been set. There is no default card type.

Note Mixing of T1 and E1 interface types is not supported. All ports on the interface module must be of the same type.

To set the card type for the T1/E1 interface module, complete these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 **card type** {**e1** | **t1**} *slot/subslot*

Example:

```
Router(config)# card type e1 0/3
```

Sets the serial mode for the interface module:

- t1—Specifies T1 connectivity of 1.536 Mbps. B8ZS is the default linecode for T1.
- e1—Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 1.984 Mbps in framed mode and 2.048 Mbps in unframed E1 mode.
- *slot subslot* —Specifies the location of the interface module.

Step 3 **exit**

Example:

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

Exits configuration mode and returns to the EXEC command interpreter prompt.

Enabling T1 Controller

Note T1/T3 or E1/E3 does not require any license.

To enable T1 controller:

```
enable
configure terminal
controller mediatype 0/4/0
mode t1
end
```

Configuring the Controller

To create the interfaces for the T1/E1 interface module, complete these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 **controller** {**t1** | **e1**} *slot/subslot/port*

Example:

```
Router(config)# controller t1 0/3/0
```

Selects the controller to configure and enters controller configuration mode.

- t1—Specifies the T1 controller.
- e1—Specifies the E1 controller.
- *slot/subslot/port*—Specifies the location of the interface.

Note The slot number is always 0.

Step 3 **clock source** {**internal** | **line**}

Example:

```
Router(config-controller)# clock source internal
```

Sets the clock source.

Note The clock source is set to internal if the opposite end of the connection is set to line and the clock source is set to line if the opposite end of the connection is set to internal.

- internal—Specifies that the internal clock source is used.
- line—Specifies that the network clock source is used. This is the default for T1 and E1.

Step 4 **linecode** {**ami** | **b8zs** | **hdb3**}

Example:

```
Router(config-controller)# linecode ami
```

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for T1 controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (HDB3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Step 5 For T1 Controllers:

Example:

```
framing {sf | esf}
```

Example:

```
Router(config-controller)# framing sf
```

Example:

```
For E1 Controllers:
```

Example:

```
framing {crc4 | no-crc4}
```

Example:

```
Router(config-controller)# framing crc4
```

Selects the framing type.

- sf—Specifies Super Frame as the T1 frame type.
- esf—Specifies Extended Super Frame as the T1 frame type. This is the default for E1.
- crc4—Specifies CRC4 as the E1 frame type. This is the default for E1.
- no-crc4—Specifies no CRC4 as the E1 frame type.

Step 6 **cablelength** {**long** | **short**}

Example:

```
Router(config-controller)# cablelength long
```

To fine-tune the pulse of a signal at the receiver for an E1 cable, use the **cablelength** command in controller configuration mode.

Step 7 **exit**

Example:

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

Exits configuration mode and returns to the EXEC command interpreter prompt.

Verifying Controller Configuration

To verify the controller configuration, use the show controllers command :

```
Router# show controllers t1 0/3/0 brief
T1 0/3/0 is up.
  Applique type is A900-IMA16D
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  Data in current interval (230 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Total Data (last 24 hours)
     136 Line Code Violations, 63 Path Code Violations,
     0 Slip Secs, 6 Fr Loss Secs, 4 Line Err Secs, 0 Degraded Mins,
     7 Errored Secs, 1 Bursty Err Secs, 6 Severely Err Secs, 458 Unavail Secs
     2 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

Optional Configurations

There are several standard, but optional, configurations that might be necessary to complete the configuration of your T1/E1 interface module.

Configuring Framing

Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. To configure framing, use the following commands.

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 **controller** {**t1** | **e1**} *slot/subslot/port*

Example:

```
Router(config)# controller t1 0/3/0
```

Selects the controller to configure.

- t1—Specifies the T1 controller.
- e1—Specifies the E1 controller.
- slot/subslot/port—Specifies the location of the controller.

Note The slot number is always 0.

Step 3 For T1 controllers

Example:

```
framing {sf | esf}
```

Example:

```
Router(config-controller)# framing sf
```

Example:

Example:

```
For E1 controllers
```

Example:

```
framing {crc4 | no-crc4}
```

Example:

```
Router(config-controller)# framing crc4
```

Sets the framing on the interface.

- sf—Specifies Super Frame as the T1 frame type.
- esf—Specifies Extended Super Frame as the T1 frame type. This is the default for T1.
- crc4—Specifies CRC4 frame as the E1 frame type. This is the default for E1.

- no-crc4—Specifies no CRC4 as the E1 frame type.

Step 4 **exit**

Example:

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

Exits configuration mode and returns to the EXEC command interpreter prompt.

Verifying Framing Configuration

Use the show controllers command to verify the framing configuration:

```
Router# show controllers t1 0/3/0 brief
T1 0/3/0 is up.
  Applique type is A900-IMA16D
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is ESF, Line Code is B8ZS
, Clock Source is Line.
  Data in current interval (740 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

Setting an IP Address

To set an IP address for the serial interface, complete these steps:

You can also set an IP address using an IMA or CEM configuration.

Procedure

Step 1 **interface serial** *0/subslot/port:channel-group*

Example:

```
Router(config)# interface serial 0/0/1:0
```

Selects the interface to configure from global configuration mode.

- *subslot*—**Specifies the subslot in which the T1/E1 interface module is installed.**
- *port* —Specifies the location of the controller. The port range for T1 and E1 is 1 to 16.
- *channel-group* —Specifies the channel group number configured on the controller. For example: interface serial 0/0/1:1.

Step 2 **ip address** *address mask*

Example:

```
Router(config-if)# ip address 192.0.2.1 255.255.255.0
```

Sets the IP address and subnet mask.

- *address* —Specify the IP address.
- *mask* —Specify the subnet mask.

Step 3 **exit**

Example:

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

Exits configuration mode and returns to the EXEC command interpreter prompt.

What to do next

Note IPV4 routing protocols, such as *eigrp* , *ospf* , *bgp* , and *rip* , are supported on serial interfaces.

Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic.

Note L2TPv3 encapsulation is *not* supported.

To set the encapsulation method, use the following commands:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Example:

Enters global configuration mode.

Step 2 **interface serial** *0/subslot/port:channel-group*

Example:

```
Router(config)# interface serial 0/0/1:0
```

Example:

Selects the interface to configure from global configuration mode.

- *subslot***—Specifies the subslot in which the T1/E1 interface module is installed.**
- *port* —Specifies the location of the controller. The port range for T1 and E1 is 1 to 16.
- *channel-group* —Specifies the channel group number configured on the controller. For example: interface serial 0/0/1:1.

Step 3 **encapsulation** {**hdlc** | **ppp**}

Example:

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

Set the encapsulation method on the interface.

- **hdlc**—High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces.
- **ppp**—Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.

Step 4 **exit**

Example:

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

Exits configuration mode and returns to the EXEC command interpreter prompt.

Verifying Encapsulation

Use the **show interfaces serial** command to verify encapsulation on the interface:

```
Router#  show  interfaces  serial
  0/0/1:0
Serial0/0/1:0 is up, line protocol is up
  Hardware is Multichannel T1
  MTU 1500 bytes, BW 1536 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC
, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     60 packets input, 8197 bytes, 0 no buffer
     Received 39 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
64 packets output, 8357 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions
```

Configuring the CRC Size for T1 Interfaces

All T1/E1 serial interfaces use a 16-bit cyclic redundancy check (CRC) by default, but also support a 32-bit CRC. CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used CRC throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE 802 and as an option by some point-to-point transmission standards.

To set the length of the cyclic redundancy check (CRC) on a T1 interface, use these commands:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Example:

Enters global configuration mode.

Step 2 **interface serial** *0/subslot/port:channel-group*

Example:

```
Router(config)# interface serial 0/0/1:0
```

Example:

Selects the interface to configure from global configuration mode.

- *number* —Specifies the location of the controller. The number range for T1 and E1 is 1 to 16.
- *channel-group* —Specifies the channel group number configured on the controller. For example: interface serial 0/1:1.

Step 3 **crc** {**16** | **32**}

Example:

```
Router(config-if)# crc 16
```

Selects the CRC size in bits.

- 16—16-bit CRC. This is the default.

- 32—32-bit CRC.

Note Moving from CRC 16 to 32 bit (and vice-versa) is not supported.

Step 4 **exit**

Example:

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

Exits configuration mode and returns to the EXEC command interpreter prompt.

Verifying the CRC Size

Use the **show interfaces serial** command to verify the CRC size set on the interface:

```
Router#  show  interfaces  serial  0/0/1:0
Serial0/0/1:0 is up, line protocol is up
  Hardware is Multichannel T1
  MTU 1500 bytes, BW 1536 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16
, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     60 packets input, 8197 bytes, 0 no buffer
     Received 39 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     64 packets output, 8357 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
```

Configuring a Channel Group

Follow these steps to configure a channel group:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 **controller** {**t1** | **e1**} *slot/subslot/port*

Example:

```
Router(config)# controller t1 0/3/0
```

Select the controller to configure and enter global configuration mode.

Step 3 **channel-group** [**t1** | **e1**] *number* {**timeslots** *range* | **unframed**} [**speed** {**56** | **64**}]

Example:

```
Router(config-controller)# channel-group t1 1timeslots 1 | unframed speed 56
```

Defines the time slots that belong to each T1 or E1 circuit.

- *number*— Channel-group number. When configuring a T1 data line, channel-group numbers can be values from 1 to 28. When configuring an E1 data line, channel-group numbers can be values from 0 to 30.
- **timeslots** *range*— One or more time slots or ranges of time slots belonging to the channel group. The first time slot is numbered 1. For a T1 controller, the time slot range is from 1 to 24. For an E1 controller, the time slot range is from 1 to 31.
- **unframed**—Unframed mode (G.703) uses all 32 time slots for data. None of the 32 time slots are used for framing signals.
- **speed**—(Optional) Specifies the speed of the underlying DS0s in kilobits per second. Valid values are 56 and 64.

Note The default is 64. Speed is not mentioned in the configuration.

Note Each channel group is presented to the system as a serial interface that can be configured individually.

Note Once a channel group has been created with the channel-group command, the channel group cannot be changed without removing the channel group. To remove a channel group, use the **no** form of the **channel-group** command.

Note The unframed option is not currently supported.

Note DS0-level channelization is not currently supported.

Step 4 **exit**

Example:

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

Exits configuration mode and returns to the EXEC command interpreter prompt.

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
copy running-config startup-config	Writes the new configuration to NVRAM.

For information about managing your system images and configuration files, refer to the Cisco IOS Configuration Fundamentals Configuration Guide and Cisco IOS Configuration Fundamentals Command Reference publications.

Troubleshooting E1 and T1 Controllers

You can use the following methods to troubleshoot the E1 and T1 controllers using Cisco IOS software:

- Setting Loopbacks, on page 73
- Runing Bit Error Rate Testing, on page 74

Setting Loopbacks

The following sections describe how to set loopbacks:

Setting a Loopback on the E1 Controller

To set a loopback on the E1 controller, perform the first task followed by any of the following tasks beginning in global configuration mode:

Command	Purpose
configure terminal	Enters global configuration mode.
controller e1 *slot/subslot/port*	Select the E1 controller and enter controller configuration mode.The slot number is always 0.
loopback diag	Set a diagnostic loopback on the E1 line.
loopback network {**line** | **payload**}	Set a network payload loopback on the E1 line.
end	Exit configuration mode when you have finished configuring the controller.

Setting a Loopback on the T1 Controller

You can use the following loopback commands on the T1 controller in global configuration mode:

Task	Command
controller t1 *slot/subslot/port*	Selects the T1 controller and enter controller configuration mode The slot number is always 0.
loopback diag	Sets a diagnostic loopback on the T1 line.
loopback local {**line** | **payload**}	Sets a local loopback on the T1 line. You can select to loopback the line or the payload.
loopback remote iboc	Sets a remote loopback on the T1 line. This loopback setting will loopback the far end at line or payload, using IBOC (in band bit-orientated code) or the Extended Super Frame (ESF) loopback codes to communicate the request to the far end.
end	Exits configuration mode when you have finished configuring the controller.

Note To remove a loopback, use the **no loopback** command.

Table 9: Loopback Descriptions

Loopback	Description
loopback diag	Loops the outgoing transmit signal back to the receive signal. This is done using the diagnostic loopback feature in the interface module's PMC framer. The interface module transmits AIS in this mode. Set the **clock source** command to **internal** for this loopback mode.
loopback local	Loops the incoming receive signal back out to the transmitter. You can specify whether to use the **line** or **payload**.
local line	The incoming signal is looped back in the interface module using the framer's line loopback mode. The framer does not reclock or reframe the incoming data. All incoming data is received by the interface module driver.
local payload	Loops the incoming signal back in the interface module using the payload loopback mode of the framer. The framer reclocks and reframes the incoming data before sending it back out to the network. When in payload loopback mode, an all 1s data pattern is received by the local HDLC receiver and the clock source is automatically set to line (overriding the **clock source** command). When the payload loopback is ended, the clock source returns to the last setting selected by the **clock source** command.
loopback remote iboc	Attempts to set the far-end T1 interface into line loopback. This command sends an in-band bit-oriented code to the far-end to cause it to go into line loopback. This command is available when using ESF or SF framing mode.
network line	Loops the incoming signal back in the interface module using the line loopback mode of the framer. The framer does not reclock or reframe the incoming data. All incoming data is received by the interface module driver.
network payload	Loops the incoming signal back using the payload loopback mode of the framer. The framer reclocks and reframes the incoming data before sending it back out to the network. When in payload loopback mode, an all 1s data pattern is received by the local HDLC receiver, and the clock source is automatically set to line (overriding the **clock source** command). When the payload loopback is ended, the clock source returns to the last setting selected by the **clock source** command.

Runing Bit Error Rate Testing

Bit error rate testing (BERT) is supported on each of the E1 or T1 links. The BERT testing is done only over a framed E1 or T1 signal and can be run only on one port at a time.

The interface modules contain onboard BERT circuitry. With this, the interface module software can send and detect a programmable pattern that is compliant with CCITT/ITU O.151, O.152, and O.153 pseudo-random and repetitive test patterns. BERTs allows you to test cables and signal problems in the field.

When running a BER test, your system expects to receive the same pattern that it is transmitting. To help ensure this, two common options are available:

- Use a loopback somewhere in the link or network
- Configure remote testing equipment to transmit the same BERT test pattern at the same time

To run a BERT on an E1 or T1 controller, perform the following optional tasks beginning in global configuration mode:

Task	Command
controller {**e1** | **t1**} *slot/subslot/port*	Selects the E1 or T1 controller and enters controller configuration mode. The slot number is always 0.
bert pattern 0s | **1s** | **2^11** | **2^15** | **2^20-O153** | **2^20-QRSS** | **2^23** | **alt-0-1**} **interval** *minutes*	Specifies the BERT pattern for the E1 or T1 line and the duration of the test in minutes. The valid range is 1 to 1440 minutes. **Note** Only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported.
end	Exit configuration mode when you have finished configuring the controller.
show controllers {**e1** | **t1**} *slot/subslot/port*	Displays the BERT results.

The following keywords list different BERT keywords and their descriptions.

Caution Currently only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported.

Table 10: BERT Pattern Descriptions

Keyword	Description
0s	Repeating pattern of zeros (...000...).
1s	Repeating pattern of ones (...111...).
2^11	Pseudo-random test pattern that is 2,048 bits in length.
2^15	Pseudo-random O.151 test pattern that is 32,768 bits in length.
2^20-O153	Pseudo-random O.153 test pattern that is 1,048,575 bits in length.
2^20-QRSS	Pseudo-random QRSS O.151 test pattern that is 1,048,575 bits in length.
2^23	Pseudo-random 0.151 test pattern that is 8,388,607 bits in length.

Keyword	Description
alt-0-1	Repeating alternating pattern of zeros and ones (...01010...).

Both the total number of error bits received and the total number of bits received are available for analysis. You can select the testing period from 1 minute to 24 hours, and you can also retrieve the error statistics anytime during the BER test.

Note To terminate a BERT test during the specified test period, use the **no bert** command.

You can view the results of a BERT test at the following times:

- After you terminate the test using the **no bert** command
- After the test runs completely
- Anytime during the test (in real time)

Monitoring and Maintaining the T1/E1 Interface Module

After configuring the new interface, you can monitor the status and maintain the interface module by using **show** commands. To display the status of any interface, complete any of the following tasks in **EXEC** mode:

Task	Command
show controllers {**e1** | **t1**} [*slot/port-adapter/port/e1-line*] [**brief**	Displays the status of the E1 or T1 controller.
show interface serial*slot/subslot/port*	Displays statistics about the serial information for a specific E1 or T1 channel group. Valid values are 0 to 30 for E1 and 0 to 23 for T1.
clear counters serial *slot/subslot/port*	Clears the interface counters

Note To change the T1/E1 card type configuration, use the **no card type** command and reload the router.

AIS on Core Failure

AIS stands for Alarm Indication Signal. Prior to Cisco IOS XE Fuji Release 16.7.1, the PDH AIS alarms were generated only when the CE would go down and an event was set in the CEM control-word by the remote provider edge (PE). AIS alarms were not generated when the pesudowire went down. Now, AIS alarm are generated when the pesudowire goes down.

This feature is only supported on the Cisco ASR 900 RSP2 module, for 8-port T1/E1 and 16-port T1/E1 interface modules and only for unframed E1 mode (SAToP) type.

Limitations of AIS

- AIS is not supported on CESoP and CEM over UDP.
- AIS is not supported on T1 mode. It is only supported on E1 mode.
- AIS is not supported on the 4-port OC3/STM-1 (OC-3) interface module (IM) and 32-port T1/E1 IM.
- AIS is supported only for MPLS core.
- AIS is not supported in pseudowire HSPW mode, when **graceful-restart** command is enabled.
- Removing the MPLS IP address from the core interfaces results in a delay of 10-12 minutes to notify the peer end. This depends on the negotiated forwarding hold timer between the routers, which is the least value of the configured LDP GR forwarding hold timer of the two routers.
- Supported CEM class range of de-jitter buffer size is between 1 to 32 ms.
- If the **shutdown unpowered** command is used to shut down the IM, an OIR must be performed to trigger the AIS alarms..

Core Failure Event Detection

AIS configuration is used to detect core defects. The core failure is detected in the following events:

- Shutdown of the PE controller or tug level.
- Removing the cross-connect feature.
- Removal of Gigabit Ethernet configuration, CEM configuration, controller configuration, or OSPF configuration.
- Shut on OSPF, CEM group, cross-connect, or Gigabit Ethernet interface.
- CE1 controller shut—AIS alarm is seen on the remote CE.
- PE1 controller shut—AIS alarm is seen on the remote CE.
- PE1 core shut—AIS alarm is seen on both the CEs.
- PE2 core shut—AIS alarm is seen on both the CEs.
- Pesudowire down—AIS alarm is seen on both the CEs.
- Core IGP down—AIS alarm is seen on both the CEs.
- Core LDP down—AIS alarm is seen on both the CEs.

Configuring AIS for Core Failure

When you enable the AIS, Plesiochronous Digital Hierarchy (PDH) AIS alarm is supported for core failure events on the 8-port T1/E1 and 16-port T1/E1 interface modules. When a core failure is detected due to any event, core flap flag is updated and the core flap event sends an event, which asserts an AIS. When the AIS is not enabled, core failure events are ignored.

Use the following procedure to enable AIS:

```
Router> enable
Router#configure terminal
```

```
Router(config)#controller t1 0/1/2
Router(config-controller)#ais-core-failure
```

Verifying AIS Configuration

Use the **show run | sec** command to verify the configuration of AIS:

```
Router(config-controller)#show run | sec 0/3/0
controller E1 0/3/0
 ais-core-failure
 framing unframed
  cem-group 30 unframed
interface CEM0/3/0
```

Example: AIS Trigger

The following example shows a sample configuration of a controller O/P when an AIS is triggered:

```
Router#show controller e1 0/2/1
E1 0/2/1 is down.
Applique type is A900-IMA16D
Cablelength is Unknown
Transmitter is sending remote alarm.
Receiver is getting AIS. <<<<<<<<<<<<< This is AIS alarm received
ais-shut is not set
alarm-trigger is not set
Framing is crc4, Line Code is HDB3, Clock Source is Line.
BER thresholds: SF = 10e-5 SD = 10e-5
International Bit: 1, National Bits: 11111
Data in current interval (0 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
1 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display the configuration settings, use the **show interfaces serial** and the **show controllers serial** commands to get detailed information on a per-port basis for your T1/E1 interface module.

Verifying Per-Port Interface Status

To view detailed interface information on a per-port basis for the T1/E1 interface module, use the **show interfaces serial** command.

```
Router# show interfaces serial 0/0/1:0
Serial0/0/1:0 is up, line protocol is up
  Hardware is SPA-8XCHT1/E1
  Internet address is 79.1.1.2/16
  MTU 1500 bytes, BW 1984 Kbit, DLY 20000 usec,
     reliability 255/255, txload 240/255, rxload 224/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Last input 3d21h, output 3d21h, output hang never
  Last clearing of ''show interface'' counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 2998712
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1744000 bits/sec, 644 packets/sec
  5 minute output rate 1874000 bits/sec, 690 packets/sec
     180817311 packets input, 61438815508 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
     180845200 packets output, 61438125092 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions no alarm present
  Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags 2
```

Configuration Examples

This section includes the following configuration examples:

Example: Framing and Encapsulation Configuration

The following example sets the framing and encapsulation for the controller and interface:

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 2/0/0
!
! Specify the framing method
!
Router(config-controller)# framing esf
!
! Exit controller configuration mode and return to global configuration mode
!
Router(config-controller)# exit
!
! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 2/0/0:0
!
! Specify the encapsulation protocol
!
Router(config-if)# encapsulation ppp
!
! Exit interface configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

Example: CRC Configuration

The following example sets the CRC size for the interface:

```
! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 2/0/0:0
```

```
!
! Specify the CRC size
!
Router(config-if)# crc 32
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

Example: Facility Data Link Configuration

The following example configures Facility Data Link:

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 2/0/0
!
! Specify the FDL specification
!
Router(config-controller)#
fdl ansi
!
! Exit controller configuration mode and return to global configuration mode
!
Router(config-controller)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

Example: Invert Data on the T1/E1 Interface

The following example inverts the data on the serial interface:

```
! Enter global configuration mode
!
Router# configure terminal
!
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/3:0
!
! Configure invert data
!
Router(config-if)# invert data
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

CHAPTER 7

Dying Gasp Support for Loss of Power Supply via SNMP, Syslog and Ethernet OAM

Dying Gasp—One of the following unrecoverable condition has occurred:

- Interface error-disable
- Reload
- Power failure or removal of power supply cable

This type of condition is vendor specific. An Ethernet Operations, Administration, and Maintenance (OAM) notification about the condition may be sent immediately.

Prerequisites for Dying Gasp Support

Dying Gasp via ethernet OAM is not supported on Cisco RSP3 module.

You must enable Ethernet OAM on interface that requires Dying Gasp notification via Ethernet OAM. For more information, see *Enabling Ethernet OAM on an interface*.

You must enable SNMP global configurations to get notification via SNMP trap. For more information, see *Configuration Examples for Dying Gasp support via SNMP*.

Restrictions for Dying Gasp Support

- The Dying Gasp feature is not supported if you remove the power supply unit (PSU) from the system.
- SNMP trap is sent only on power failure that results in the device to shut down.
- The Dying Gasp support feature cannot be configured using CLI. To configure hosts using SNMP, refer to the SNMP host configuration examples below.

- Dying Gasp via SNMP Trap is *not* supported on Management Port Gig0/Management-interface vrf on Cisco RSP3 module and Cisco ASR 920 routers.

Configuration Examples for Dying Gasp Support

Configuring SNMP Community Strings on a Router

Setting up the community access string to permit access to the SNMP:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server community public RW
Router(config)# exit
```

For more information on command syntax and examples, refer to the Cisco IOS Network Management Command Reference.

Configuring SNMP-Server Host Details on the Router Console

Specifying the recipient of a SNMP notification operation:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host X.X.X.XXX vrf mgmt-intf version 2c public udp-port 9800
```

Router(config)# exit

For more information on command syntax and examples, refer to the Cisco IOS Network Management Command Reference.

Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations

Note You can configure up to five different SNMP server host/port configurations.

Environmental Settings on the Network Management Server

```
setenv SR_TRAP_TEST_PORT=UDP port
setenv SR_UTIL_COMMUNITY=public
setenv SR_UTIL_SNMP_VERSION=v2c
setenv SR_MGR_CONF_DIR=Path to the executable snmpinfo.DAT file
```

The following example shows SNMP trap configuration on three hosts:

Configuration example for the first host:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)# snmp-server host 7.0.0.149 vrf Mgmt-intf version 2c public udp-port 6264
Configuration example for the second host:
Router(config)#
Router(config)# snmp-server host 7.0.0.152 vrf Mgmt-intf version 2c public udp-port 9988
Configuration example for the third host:
Router(config)# snmp-server host 7.0.0.166 vrf Mgmt-intf version 2c public udp-port 9800
Router(config)#
Router(config)# ^Z
Router#
```

After performing a power cycle, the following output is displayed on the router console:

Note This is not supported on Cisco RSP1 and Cisco RSP2 modules.

```
Router#
System Bootstrap, Version 15.3(2r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012 by cisco Systems, Inc.
Compiled Wed 17-Oct-12 15:00
Current image running: Boot ROM1
Last reset cause: PowerOn
UEA platform with 2097152 Kbytes of main memory
rommon 1 >
=======================================
Dying Gasp Trap Received for the Power failure event:
-----------------------------------------------------
  Trap on Host1
++++++++++++++
snmp-server host = 7.0.0.149 (nms1-lnx)  and SR_TRAP_TEST_PORT=6264
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
--------------------------------------------------------------------
  Trap on Host2
+++++++++++++
snmp-server host = 7.0.0.152  (nms2-lnx)  and SR_TRAP_TEST_PORT=9988
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
--------------------------------------------------------------
   Trap on Host3
++++++++++++++
snmp-server host = 7.0.0.166  (erbusnmp-dc-lnx)  and SR_TRAP_TEST_PORT=9800
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
```

```
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
```

Message Displayed on the Peer Router on Receiving Dying Gasp Notification

```
001689: *May 30 14:16:47.746 IST: %ETHERNET_OAM-6-RFI: The client on interface Gi4/2 has
received a remote failure indication from its remote peer(failure reason = remote client
power failure action = )
```

Displaying SNMP Configuration for Receiving Dying Gasp Notification

Use the show running-config command to display the SNMP configuration for receiving dying gasp notification:

```
Router# show running-config | i snmp
snmp-server community public RW
snmp-server host 7.0.0.149 vrf Mgmt-intf version 2c public udp-port 6264
snmp-server host 7.0.0.152 vrf Mgmt-intf version 2c public udp-port 9988
snmp-server host 7.0.0.166 vrf Mgmt-intf version 2c public udp-port 9800
Router#
```

Dying GASP via SNMP Trap Support on Cisco RSP3 Module

Dying GASP via SNMP trap feature is supported on Cisco RSP3 module.

no packets can be processed in this time by CPU. To avoid this, this feature pre-constructs and installs the event packet in FPGA. When FPGA receives the power failure notificaion, it transfers the pre-constructed packet and thus the packet is forwarded to the required egress interface.

The feature helps to quickly notify a network administrator whenever a node undergoes power shutdown. The node undergoing power shutdown sends a SNMP DG trap message to the configured SNMP server .

The feature is supported on global MPLS and L3VPN. It uses UDP port 49151 as source port and 162 as destination port.

Restrictions for Dying GASP via SNMP Trap Support on Cisco RSP3 Module

- The feature is enabled by default in Cisco RSP3C Port Expansion Mode when the channelized IMs are inserted in the device with the following conditions:

  If the above-mentioned IMs are not inserted in the above-mentioned slots, you can still connect by enabling the following command in the global configurations:

  platform dying-gasp-port-enable

Note The above command only supported in Cisco RSP3C Port Expansion Mode.

But, some IMs in some slot can no longer be online. The enabled command checks if these slots are free of those IMs, if they are not, it rejects the implementation and error message is displayed. The same scenario is experienced when the command is enabled and incompatible IM is inserted. For information on incompatible IMs, refer the IM Compatibility Tool .

- Only SNMP Dying Gasp traps are received in an event of power failure.

  The SNMP Dying Gasp traps are *only* received for the first five configured SNMP hosts. Only five SNMP server hosts are notified about SNMP trap.

- Generation of SNMP trap for host via management VRF for a Dying GASP event is not supported in Cisco RSP3 Module.

- Reachability to the host must be present and Address Resolution Protocol (ARP) must be resolved before the event.

- Dying GASP support for loss of power supply via syslog and Ethernet OAM is not supported.

Enabling Dying GASP Support on Cisco RSP3 Module

To enable Dying GASP feature for Cisco RSP3 module in Cisco RSP3C Port Expansion Mode:

```
enable
configure terminal
platform dying-gasp-port-enable
end
```

To enable the feature in Cisco RSP3C XFI-Pass Through Mode:

```
enable
configure terminal
license feature service-offload enable
Reload the device. If present, IM  goes out of serive. If not, deactivate the IM.
license feature service-offload bandwidth 10gbps npu-[0 | 1]
Reload the device.
end
```

Verifying SNMP Host Configuration

Use **show snmp host** command to verify all SNMP hosts configured.

```
#show snmp host
Notification host: 20.20.20.21  udp-port: 162   type: trap
user: public    security model: v2c

Notification host: 30.30.30.31  udp-port: 162   type: trap
user: public    security model: v2c

Notification host: 5000::2      udp-port: 162   VRFName: vrf1   type: trap
user: public    security model: v3 noauth

Notification host: 6000::2      udp-port: 162   VRFName: vrf1   type: trap
user: public    security model: v3 noauth
```

```
Notification host: 8000::2      udp-port: 162   type: trap
user: public    security model: v2c
```

Verifying SNMP Configurations

Use **show running | i snmp** command to verify all SNMP hosts configured.

```
#show running | i snmp
snmp-server group public v3 noauth
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source Loopback0
snmp-server host 20.20.20.21 version 2c public
snmp-server host 30.30.30.31 version 2c public
snmp-server host 5000::2 vrf vrf1 version 3 noauth public
snmp-server host 6000::2 vrf vrf1 version 3 noauth public
snmp-server host 8000::2 version 2c public
```

CHAPTER 8

Tracing and Trace Management

This chapter contains the following sections:

Tracing Overview

Tracing is a function that logs internal events. Trace files are automatically created and saved to the tracelogs directory on the harddisk: file system on the chassis, which stores tracing files in bootflash:. Trace files are used to store tracing data.

Note The logs in the bootflash are stored in compressed format with .gz file extension. Use the archiving tools such as gunzip, gzip, 7-zip to extract the files.

- If the sytem reloads unexpectedly, some of the files may not be in compressed format.
- Extraction of log files may lead to time hogs or CPU logs. We recommend to perform this by copying the files to the PC.
- Extraction of files *cannot* be performed at the IOS prompt.
- Log files not handled by the bootflash trace are *not* stored in the compressed format (for example, system_shell_R*.log).

The contents of trace files are useful for the following purposes:

- Troubleshooting—If a chassis is having an issue, the trace file output may provide information that is useful for locating and solving the problem. Trace files can almost always be accessed through diagnostic mode even if other system issues are occurring.
- Debugging—The trace file outputs can help users get a more detailed view of system actions and operations.

How Tracing Works

The tracing function logs the contents of internal events on the chassis. Trace files with all trace output for a module are periodically created and updated and are stored in the tracelog directory. Trace files can be erased from this directory to recover space on the file system without impacting system performance.

The most recent trace information for a specific module can be viewed using the **show platform software trace message** privileged EXEC and diagnostic mode command. This command can be entered to gather trace log information even during an IOS failure because it is available in diagnostic mode.

Trace files can be copied to other destinations using most file transfer functions (such as FTP, TFTP, and so on) and opened using a plaintext editor.

Tracing cannot be disabled on the chassis. Trace levels, however, which set the message types that generate trace output, are user-configurable and can be set using the **set platform software trace** command. If a user wants to modify the trace level to increase or decrease the amount of trace message output, the user should set a new tracing level using the **set platform software trace** command. Trace levels can be set by process using the **all-modules** keyword within the **set platform software trace** command, or by module within a process. See the **set platform software trace** command reference for more information on this command, and the Tracing Levels, on page 88 of this document for additional information on tracing levels.

Tracing Levels

Tracing levels determine how much information about a module should be stored in the trace buffer or file.

Table 11: Tracing Levels and Descriptions, on page 88 shows all of the trace levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

Table 11: Tracing Levels and Descriptions

Trace Level	Level Number	Description
Emergency	0	The message is regarding an issue that makes the system unusable.
Alert	1	The message is regarding an action that must be taken immediately.
Critical	2	The message is regarding a critical condition. This is the default setting.
Error	3	The message is regarding a system error.
Warning	4	The message is regarding a system warning
Notice	5	The message is regarding a significant issue, but the router is still working normally.
Informational	6	The message is useful for informational purposes only.
Debug	7	The message provides debug-level output.
Verbose	8	All possible tracing messages are sent.

Trace Level	Level Number	Description
Noise	-	All possible trace messages for the module are logged. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.

Trace level settings are leveled, meaning that every setting will contain all messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3(error) ensures that the trace file will contain all output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (warning) will ensure that all trace output for the specific module will be included in that trace file.

The default tracing level for every module on the chassis is notice.

All trace levels are not user-configurable. Specifically, the alert, critical, and notice tracing levels cannot be set by users. If you wish to trace these messages, set the trace level to a higher level that will collect these messages.

When setting trace levels, it is also important to remember that the setting is not done in a configuration mode, so trace level settings are returned to their defaults after every router reload.

Caution Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to this level or higher should be done with discretion.

Caution Setting a large number of modules to high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

Viewing a Tracing Level

By default, all modules on the chassis are set to notice. This setting will be maintained unless changed by a user.

To see the tracing level for any module on the chassis, enter the **show platform software trace level** command in privileged EXEC or diagnostic mode.

In the following example, the **show platform software trace level** command is used to view the tracing levels of the Forwarding Manager processes on the active RSP:

```
Router# show platform software trace level forwarding-manager rp active
Module Name                     Trace Level
-----------------------------------------------
acl                             Notice
binos                           Notice
binos/brand                     Notice
bipc                            Notice
bsignal                         Notice
btrace                          Notice
```

```
cce                             Notice
cdllib                          Notice
cef                             Notice
chasfs                          Notice
chasutil                        Notice
erspan                          Notice
ess                             Notice
ether-channel                   Notice
evlib                           Notice
evutil                          Notice
file_alloc                      Notice
fman_rp                         Notice
fpm                             Notice
fw                              Notice
icmp                            Notice
interfaces                      Notice
iosd                            Notice
ipc                             Notice
ipclog                          Notice
iphc                            Notice
ipsec                           Notice
mgmte-acl                       Notice
mlp                             Notice
mqipc                           Notice
nat                             Notice
nbar                            Notice
netflow                         Notice
om                              Notice
peer                            Notice
qos                             Notice
route-map                       Notice
sbc                             Notice
services                        Notice
sw_wdog                         Notice
tdl_acl_config_type             Notice
tdl_acl_db_type                 Notice
tdl_cdlcore_message             Notice
tdl_cef_config_common_type      Notice
tdl_cef_config_type             Notice
tdl_dpidb_config_type           Notice
tdl_fman_rp_comm_type           Notice
tdl_fman_rp_message             Notice
tdl_fw_config_type              Notice
tdl_hapi_tdl_type               Notice
tdl_icmp_type                   Notice
tdl_ip_options_type             Notice
tdl_ipc_ack_type                Notice
tdl_ipsec_db_type               Notice
tdl_mcp_comm_type               Notice
tdl_mlp_config_type             Notice
tdl_mlp_db_type                 Notice
tdl_om_type                     Notice
tdl_ui_message                  Notice
tdl_ui_type                     Notice
tdl_urpf_config_type            Notice
tdllib                          Notice
trans_avl                       Notice
uihandler                       Notice
uipeer                          Notice
uistatus                        Notice
urpf                            Notice
vista                           Notice
wccp                            Notice
```

Setting a Tracing Level

To set a tracing level for any module on the chassis, or for all modules within a process, enter the **set platform software trace** privileged EXEC and diagnostic mode command.

In the following example, the trace level for the ACL module in the Forwarding Manager of the ESP processor in slot 0 is set to info.

set platform software trace forwarding-manager F0 acl info

See the **set platform software trace** command reference for additional information about the options for this command.

Viewing the Content of the Trace Buffer

To view the trace messages in the trace buffer or file, enter the **show platform software trace message** privileged EXEC and diagnostic mode command.

In the following example, the trace messages for the Host Manager process in Route Switch Processor slot 0 are viewed using the **show platform software trace message** command:

```
Router# show platform software trace message host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
```

CHAPTER 9

Configuring and Monitoring Alarm

This chapter describes monitoring alarms, alarms filtering support and configuring external alarms for fan tray alarm port.

This chapter includes the following sections:

Monitoring Alarms

Once hardware is installed and operational, use alarms to monitor hardware status on a daily basis.

The routers are designed to send alarm notifications when problems are detected. Network administrators do not need to use show commands to poll devices on a routine basis and can monitor the network remotely. However, network administrators can perform onsite monitoring if they so choose.

Use **snmp-server enable traps alarms <severity>** command to enable the entity related Traps.

The default severity level is informational, which shows all alarms. Severity levels are defined as the following:

- 1—Critical. The condition affects service.
- 2—Major. Immediate action is needed.
- 3—Minor. Minor warning conditions.
- 4—Informational. No action is required. This is the default.

The entity notifications **ceAlarmAsserted** and **ceAlarmCleared** are used to report the condition for e.g. when a physical entity asserted or cleared an alarm.

Note Effective from Cisco IOS XE Everest 16.6.1, on RSP3 module, alarm notification is enabled on 900 watts DC power supply. There are 2 input feeds for 900 watts DC power supply, if one of the input voltage is lesser than the operating voltage, critical alarm is generated for that particular feed and clears (stops) once the voltage is restored but the power supply state remains in OK state as the other power supply is operationally up.

Network Administrator Checks Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a syslog.

Enabling the Logging Alarm Command

The logging alarm command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of alarm to log. All alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

Examples of Alarm Messages

The following alarm messages are examples of alarm messages that are sent to the console when a SPA is removed without first doing a graceful deactivation of the SPA. The alarm is cleared when the SPA is re-inserted.

SPA REMOVED

*May 18 14:50:48.540: %TRANSCEIVER-6-REMOVED: SIP0: iomd: Transceiver module removed from TenGigabitEthernet0/0/1

*May 18 14:50:49.471: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled

*May 18 14:50:49.490: %SPA_OIR-6-OFFLINECARD: SPA (A900-IMA2Z) offline in subslot 0/0

SPA RE-INSERTED

*May 18 14:52:11.803: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0

*May 18 14:52:52.807: %SPA_OIR-6-ONLINECARD: SPA (A900-IMA2Z) online in subslot 0/0

*May 18 14:52:53.543: %TRANSCEIVER-6-INSERTED: SIP0: iomd: transceiver module inserted in TenGigabitEthernet0/0/0

*May 18 14:52:53.551: %TRANSCEIVER-6-INSERTED: SIP0: iomd: transceiver module inserted in TenGigabitEthernet0/0/1

*May 18 14:52:54.780: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/0, changed state to down

*May 18 14:52:54.799: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/1, changed state to down

*May 18 14:53:06.578: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/0/1, changed state to up

*May 18 14:53:08.482: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/1, changed state to up

ALARMS for Router

To view the alarms on router, use the show facility-alarm status command. The example shows a critical alarm for Power supply along with the description:

SPA Removed

```
Router# show facility-alarm status
System Totals  Critical: 22  Major: 0  Minor: 0
Source                      Time                    Severity      Description [Index]
------                      ------                  --------      -------------------
subslot 0/0                 May 18 2016 14:50:49    CRITICAL      Active Card Removed OIR
Alarm [0]
GigabitEthernet0/1/0       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/1       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/2       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/5       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/6       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/7       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
xcvr container 0/2/0        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/2/2        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
GigabitEthernet0/2/3       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
xcvr container 0/2/4        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/2/5        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
GigabitEthernet0/2/6       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
SONET 0/3/0               May 11 2016 18:54:25   INFO          Physical Port Administrative
 State Down [36]
xcvr container 0/3/1        May 11 2016 18:53:44    INFO          Transceiver Missing [0]
xcvr container 0/3/2        May 11 2016 18:53:44    INFO          Transceiver Missing [0]
xcvr container 0/3/3        May 11 2016 18:53:44    INFO          Transceiver Missing [0]
xcvr container 0/4/0        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/1        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/2        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
GigabitEthernet0/4/3       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
xcvr container 0/4/4        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/5        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/6        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/7        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
TenGigabitEthernet0/4/8     May 11 2016 18:54:25    CRITICAL      Physical Port Link Down
[35]
```

SPA Re-Inserted

```
Router# show facility-alarm status
System Totals  Critical: 22  Major: 0  Minor: 0
Source                      Time                    Severity      Description [Index]
------                      ------                  --------      -------------------
TenGigabitEthernet0/0/0     May 18 2016 14:53:02    CRITICAL      Physical Port Link Down
[35]
GigabitEthernet0/1/0       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/1       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/2       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/5       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/6       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/7       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
xcvr container 0/2/0        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/2/2        May 11 2016 18:54:25    CRITICAL      Transceiver Missing - Link
 Down [1]
```

```
GigabitEthernet0/2/3       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
xcvr container 0/2/4       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/2/5       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
GigabitEthernet0/2/6       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
SONET 0/3/0               May 11 2016 18:54:25   INFO          Physical Port Administrative
 State Down [36]
xcvr container 0/3/1       May 11 2016 18:53:44   INFO          Transceiver Missing [0]
xcvr container 0/3/2       May 11 2016 18:53:44   INFO          Transceiver Missing [0]
xcvr container 0/3/3       May 11 2016 18:53:44   INFO          Transceiver Missing [0]
xcvr container 0/4/0       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/1       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/2       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
GigabitEthernet0/4/3       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
xcvr container 0/4/4       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/5       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/6       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/7       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
TenGigabitEthernet0/4/8    May 11 2016 18:54:25   CRITICAL      Physical Port Link Down
[35]
```

To view critical alarms specifically, use the show facility-alarm status critical command:

```
Router# show facility-alarm status critical
System Totals  Critical: 22  Major: 0  Minor: 0
Source                     Time                   Severity      Description [Index]
------                     ------                 --------      -------------------
TenGigabitEthernet0/0/0    May 18 2016 14:53:02   CRITICAL      Physical Port Link Down
[35]
GigabitEthernet0/1/0       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/1       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/2       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/5       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/6       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/1/7       May 11 2016 18:53:36   CRITICAL      Physical Port Link Down [1]
xcvr container 0/2/0       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/2/2       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
GigabitEthernet0/2/3       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
xcvr container 0/2/4       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/2/5       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
GigabitEthernet0/2/6       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
xcvr container 0/4/0       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/1       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/2       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
GigabitEthernet0/4/3       May 11 2016 18:54:25   CRITICAL      Physical Port Link Down [1]
xcvr container 0/4/4       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/5       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
```

```
xcvr container 0/4/6       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/4/7       May 11 2016 18:54:25   CRITICAL      Transceiver Missing - Link
 Down [1]
TenGigabitEthernet0/4/8    May 11 2016 18:54:25   CRITICAL      Physical Port Link Down
[35]
```

To view the operational state of the major hardware components on the router, use the show platform diag command. This example shows the Power supply P0 has failed:

```
Router# show platform diag
Chassis type: ASR903
Slot: 1, A900-RSP2A-128
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time   : 00:03:41 (00:56:24 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Sub-slot: 0/0, A900-IMA2Z
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time  : 00:04:46 (00:55:19 ago)
Sub-slot: 0/1, A900-IMA8T
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time  : 00:04:46 (00:55:19 ago)
Sub-slot: 0/2, A900-IMA8S
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time  : 00:04:46 (00:55:19 ago)
Sub-slot: 0/3, A900-IMA4OS
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:18 ago)
  Logical insert detect time  : 00:04:46 (00:55:18 ago)
Sub-slot: 0/4, A900-IMA8S1Z
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:18 ago)
  Logical insert detect time  : 00:04:46 (00:55:18 ago)
Sub-slot: 0/5, A900-IMASER14A/S
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time  : 00:04:46 (00:55:19 ago)
Slot: R0, A900-RSP2A-128
  Running state               : ok, standby
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:24:37 (00:35:28 ago)
  Software declared up time   : 00:31:28 (00:28:36 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Slot: R1, A900-RSP2A-128
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time   : 00:02:33 (00:57:31 ago)
  Became HA Active time       : 00:34:41 (00:25:23 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Slot: F0,
  Running state               : ok, standby
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:24:37 (00:35:28 ago)
  Software declared up time   : 00:31:45 (00:28:20 ago)
  Hardware ready signal time  : 00:31:39 (00:28:25 ago)
  Packet ready signal time    : 00:33:25 (00:26:40 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Slot: F1,
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time   : 00:03:23 (00:56:42 ago)
  Hardware ready signal time  : 00:03:14 (00:56:51 ago)
  Packet ready signal time    : 00:04:19 (00:55:46 ago)
  Became HA Active time       : 00:33:25 (00:26:40 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Slot: P0, Unknown
  State                       : N/A
  Physical insert detect time : 00:00:00 (never ago)
Slot: P1, A900-PWR550-A
  State                       : ok
  Physical insert detect time : 00:03:17 (00:56:48 ago)
Slot: P2, A903-FAN-E
  State                       : ok
  Physical insert detect time : 00:03:21 (00:56:44 ago)
```

Reviewing and Analyzing Alarm Messages

To facilitate the review of alarm messages, you can write scripts to analyze alarm messages sent to the console or syslog. Scripts can provide reports on events such as alarms, security alerts, and interface status.

Syslog messages can also be accessed through Simple Network Management Protocol (SNMP) using the history table defined in the CISCO-SYSLOG-MIB.

Configuring External Alarm Trigger

For Cisco ASR 902 Series Router, the fan tray includes an alarm port that maps to two (0 and 1) dry contact alarm inputs.For Cisco ASR 903 Series Router, the fan tray includes an alarm port that maps to four (0 - 3) dry contact alarm inputs.

The pins on the alarm port are passive signals and can be configured as Open (an alarm generated when current is interrupted) or Closed (an alarm is generated when a circuit is established) alarms. You can configure each alarm input as critical, major, or minor. An alarm triggers alarm LEDs and alarm messages. The relay contacts can be controlled through any appropriate third-party relay controller. The open/close configuration is an option controlled in IOS.

Approaches for Monitoring Hardware Alarms

Onsite Network Administrator Responds to Audible or Visual Alarms

An external element can be connected to a power supply using the DB-25 alarm connector on the power supply. The external element is a DC light bulb for a visual alarm and a bell for an audible alarm.

If an alarm illuminates the CRIT, MIN, or MAJ LED on the Cisco ASR 900 Series Route Processor (RP) faceplate, and a visual or audible alarm is wired, the alarm also activates an alarm relay in the power supply DB-25 connector. The bell rings or the light bulb flashes.

Clearing Audible and Visual Alarms

To clear an audible alarm, do one of the following:

- Press the Audible Cut Off button on the RP faceplate.

To clear a visual alarm, you must resolve the alarm condition. . For example, if a critical alarm LED is illuminated because an active SPA was removed without a graceful deactivation of the SPA, the only way to resolve that alarm is to replace the SPA.

Note The **clear faciltity-alarm** command is not supported. The **clear facility-alarm** command does not clear an alarm LED on the RP faceplate or turn off the DC lightbulb

How to Configure External Alarms

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**alarm-contact** *contact-number* **description** *string* **Example:** `Router(config)#alarm-contact 2 description door sensor`	(Optional) Configures a description for the alarm contact number. • The contact-number can be from 1 to 4. • The description string can be up to 80 alphanumeric characters in length and is included in any generated system messages

	Command or Action	Purpose

Step 4	**alarm-contact** {*contact-number* | **all** {**severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}}
	Example:
	`Router(config)#alarm-contact 2 severity major`
		Configures the trigger and severity for an alarm contact number or for all contact numbers.
		• Enter a contact number (1 to 4) or specify that you are configuring **all** alarms.
		• For **severity**, enter **critical**, **major**, or **minor**. If you do not configure a severity, the default is **minor**.
		• For **trigger**, enter **open** or **closed**. If you do not configure a trigger, the alarm is triggered when the circuit is **closed**.

Step 5	**exit** **Example:** `Router#exit`	Exits the configuration mode.
Step 6	**show facility-alarm status** **Example:** `Router#show facility-alarm status`	Displays configured alarms status.

Example

```
Router>enable
Router#configure terminal
Router(config)#alarm-contact 2 description door sensor
Router(config)#alarm-contact 2 severity major
Router(config)#alarm-contact 2 trigger open
Router(config)#end
Router#show facility-alarm status
System Totals  Critical: 15  Major: 0  Minor: 0

Source                     Time                   Severity      Description [Index]
------                     ------                 --------      -------------------
subslot 0/0                Sep 21 2016 15:19:55   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/1                Sep 21 2016 15:19:12   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/2                Sep 21 2016 15:16:59   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/3                Sep 21 2016 15:18:10   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/5                Sep 21 2016 15:16:11   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/6                Sep 21 2016 15:15:45   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/7                Sep 21 2016 15:14:22   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/8                Sep 21 2016 15:10:33   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/9                Sep 21 2016 12:00:43   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/10               Sep 21 2016 15:11:49   CRITICAL      Active Card Removed OIR
```

```
Alarm [0]
subslot 0/13            Sep 21 2016 14:56:35   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/14            Sep 21 2016 14:56:29   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/15            Sep 21 2016 14:56:33   CRITICAL      Active Card Removed OIR
Alarm [0]
Fan Tray Bay 0         Sep 21 2016 11:50:39   CRITICAL      Fan Tray Module Missing [0]
Router(config)#
```

Note The external alarm trigger and syslog support configuration is supported from Cisco IOS XE Release 3.13.0S.

Alarm Filtering Support

The Alarm Filtering Support in the Cisco Entity Alarm MIB feature implements the alarm filter profile capability defined in CISCO-ENTITY-ALARM-MIB. Also implemented are configuration commands to control the severity of syslog messages and SNMP notifications triggered by the alarms.

Information About Alarm Filtering Support

Overview of Alarm Filtering Support

To configure alarm filtering in the Cisco Entity Alarm MIB, you should understand the following concepts:

CISCO-ENTITY-ALARM-MIB

The CISCO-ENTITY-ALARM-MIB provides a management client with the capability to monitor alarms generated by physical entities in a network that are identified in the entPhysicalTable of the Entity-MIB (RFC 2737). Examples of these physical entities are chassis, fans, modules, ports, slots, and power supplies. The management client interfaces with an SNMP agent to request access to objects defined in the CISCO-ENTITY-ALARM-MIB.

ceAlarmGroup

The ceAlarmGroup is a group in the CISCO-ENTITY-ALARM-MIB that defines objects that provide current statuses of alarms and the capability to instruct an agent to stop (cut off) signaling for any or all external audible alarms.

Following are the objects in ceAlarmGroup:

- ceAlarmCriticalCount
- ceAlarmMajorCount
- ceAlarmMinorCount
- ceAlarmCutoff
- ceAlarmFilterProfile
- ceAlarmSeverity
- ceAlarmList

ceAlarmFilterProfileTable

The ceAlarmFilterProfileTable filters alarms according to configured alarm lists. The filtered alarms are then sent out as SNMP notifications or syslog messages, based on the alarm list enabled for each alarm type. This table is defined in the CISCO-ENTITY-ALARM-MIB and implemented in the group ceAlarmGroup.

ceAlarmFilterProfile

An alarm filter profile controls the alarm types that an agent monitors and signals for a corresponding physical entity. The ceAlarmFilterProfile object holds an integer value that uniquely identifies an alarm filter profile associated with a corresponding physical entity. When the value is zero, the agent monitors and signals all alarms associated with the corresponding physical entity.

ceAlarmHistTable:

This table contains the history of ceAlarmAsserted and ceAlarmCleared traps generated by the agent.

Each entry to the table will have physical index from entPhsicalTable and the severity of the alarm.

The ceAlarmAsserted and ceAlarmCleared trap varbinds are mostly from this table and the description from ceAlarmDescrTable.

ceAlarmDescrTable:

This table contains a description for each alarm type defined by each vendor type employed by the system.

This table has the list of possible severity levels and the description for the physical entity, Object “ceAlarmDescrSeverity” indicates the severity of an alarm (1 to 4 as above).

ceAlarmTable:

This table specifies alarm control and status information related to each physical entity contained by the system, including the alarms currently being asserted by each physical entity capable of generating alarms.

Prerequisites for Alarm Filtering Support

- SNMP is configured on your routing devices.
- Familiarity with the ENTITY-MIB and the CISCO-ENTITY-ALARM-MIB.

Restrictions for Alarm Filtering Support

- The CISCO-ENTITY-ALARM-MIB supports reporting of alarms for physical entities only, including chassis, slots, modules, ports, power supplies, and fans. In order to monitor alarms generated by a physical entity,it must be represented by a row in the entPhysicalTable .

How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications

Configuring Alarm Filtering for Syslog Messages

This task describes how to configure the alarm severity threshold for generating syslog messages. When you use this command, the alarm severity threshold is included in the running configuration and automatically applied when the configuration is reloaded.

```
enable
configure terminal
```

```
logging alarm 2
show facility-alarm status
```

Configuring Alarm Filtering for SNMP Notifications

This task describes how to configure the alarm severity threshold for generating SNMP notifications. When you use this command, the alarm severity threshold is included in the running configuration and automatically applied when the configuration is reloaded.

```
enable
configure terminal
snmp-server enable traps alarms 2
show facility-alarm status
```

Configuration Examples for Alarm Filtering Support

Configuring Alarm Filtering for Syslog Messages: Example

The following example shows how to configure an alarm filter for syslog messages:

Configuring Alarm Filtering for SNMP Notifications: Example

The following example shows how to configure an alarm filter for SNMP notifications:

```
Router# enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
 Router(config)# snmp-server enable traps alarms 2
Router(config)#
Router(config)# exit
Router# show facility-alarm status
System Totals  Critical: 2  Major: 1  Minor: 0
Source                     Time                   Severity      Description [Index]
------                     ------                 --------      -------------------
Power Supply Bay 0         Jun 07 2016 13:36:49   CRITICAL      Power Supply/FAN Module
Missing [0]
Fan Tray/Ext. ALARM:       Jun 07 2016 13:36:55   MAJOR         Fan Tray/Fan 8 Failure [15]
xcvr container 0/5/0       Jun 07 2016 13:37:43   CRITICAL      Transceiver Missing - Link
 Down [1]
xcvr container 0/5/1       Jun 07 2016 13:37:43   INFO          Transceiver Missing [0]
xcvr container 0/5/2       Jun 07 2016 13:37:43   INFO          Transceiver Missing [0]
xcvr container 0/5/3       Jun 07 2016 13:37:43   INFO          Transceiver Missing [0]
xcvr container 0/5/4       Jun 07 2016 13:37:43   INFO          Transceiver Missing [0]
xcvr container 0/5/5       Jun 07 2016 13:37:43   INFO          Transceiver Missing [0]
xcvr container 0/5/6       Jun 07 2016 13:37:43   INFO          Transceiver Missing [0]
xcvr container 0/5/7       Jun 07 2016 13:37:43   INFO          Transceiver Missing [0]
```

Facility Protocol Status Support

The routers report the protocol status using Syslog or Trap alarm notifications. Few Syslogs and Traps are not cleared when the router gets disconnected or reloaded. As a result, the alarms are not notified.

To avoid this, a new command, **show facility-protocol status**, is introduced that displays the output of the following routing protocols status at any interval of time:

- ISIS
- OSPF
- BGP
- TE Tunnels
- LDP
- Bundles
- PWs
- EVPN PWs
- CFM
- SYncE
- PTP
- HSRP
- BFD
- SensorThresholdViolations

show facility protocol status

The **`show facility-protocol status`** command helps to backup the protocols syslog information by capturing the current status of the protocols on the system.

Also, when you add a new device, the command can be used to generate a list of the outstanding protocol alarms from the device.

Restrictions

Only 14 routing protocols outputs can be displayed.

Routing Protocols Outputs

The following are the outputs of different routing protocols:

OSPF Output

```
#show facility-protocol status
==========================================================================================
Protocols   Pid  Ver  Interface                 IP-address       Status         Adj-ID
      Router-ID
==========================================================================================
OSPF       22    V2    TenGigabitEthernet0/3/4   10.0.1.2        FULL           21.22.23.25
      15.88.15.89
OSPF       100   V2   FortyGigabitEthernet0/8/1 192.168.1.1      DOWN           N/A
       100.100.100.100
```

MPLS Output

```
#show facility-protocol status
==========================================================================================
Protocols         Name   Interface                Src-IP         LDP_Neigh_IP     Status
==========================================================================================
MPLS-LDP          LDP    TenGigabitEthernet0/3/4   10.0.1.2        N/A               DOWN

MPLS-LDP          LDP    FortyGigabitEthernet0/8/1 192.168.1.1     N/A               DOWN

MPLS-LDP          LDP    GigabitEthernet0/2/0      22.1.4.1        7.7.7.7:0         UP

MPLS-LDP          LDP    GigabitEthernet0/2/4      22.0.1.1        6.6.6.6:0         UP

MPLS-LDP          LDP    Tunnel2001                5.5.5.5         2.2.2.2:0         DOWN

MPLS-LDP          LDP    Tunnel2002                5.5.5.5         2.2.2.2:0         DOWN

MPLS-LDP          LDP    Tunnel2003                5.5.5.5         2.2.2.2:0         DOWN

MPLS-LDP          LDP    Tunnel2004                5.5.5.5         2.2.2.2:0         DOWN

MPLS-LDP          LDP    Tunnel2005                5.5.5.5         2.2.2.2:0         DOWN

MPLS-LDP          LDP    Tunnel2006                5.5.5.5         2.2.2.2:0         DOWN

MPLS-LDP          LDP    Tunnel2007                5.5.5.5         2.2.2.2:0         DOWN

MPLS-LDP          LDP    Tunnel2008                5.5.5.5         2.2.2.2:0         DOWN

MPLS-LDP          LDP    Tunnel2009                5.5.5.5         2.2.2.2:0         DOWN
```

ISIS Output

```
#show facility-protocol status
==========================================================================================
Protocols      Interface       ISIS-Type         Neigh-IP        Net-ID             Status
     Sys-ID           Hold-Time
==========================================================================================
ISIS   HundredGigE0/7/0           Level-1       NA              NA                   DOWN
      NA                   NA
ISIS   HundredGigE0/7/0           Level-2       NA              NA                   DOWN
      NA                   NA
ISIS   GigabitEthernet0/3/4       Level-2       10.147.158.2    0000.0000.0158       UP
      NCS4206-158          26
ISIS   BDI72                      Level-2       10.10.72.2      0000.0000.0162       UP
      NCS4K-101-162        29
ISIS   BDI27                      Level-2       10.10.27.2      0000.0000.0162       UP
      NCS4K-101-162        23
ISIS   GigabitEthernet0/0/7       Level-2       NA              NA                   UP
      0000.0000.0152       250
ISIS   TenGigabitEthernet0/3/0    Level-2       38.206.1.3      0000.0000.0023       UP
      C101_A               28
ISIS   GigabitEthernet0/2/3       Level-2       38.76.1.3       0000.0000.0007       UP
      ASR9K_CORE           23
ISIS   Tunnel1315                 Level-2       7.7.15.2        0000.0000.0007       UP
      ASR9K_CORE           28
```

BGP Output

```
#show facility-protocol status
==========================================================================================
Protocols  LocalAS   RemoteAS  NeighborIP              Status        Up/Down Time
Remote-RID   VRF-Inst-Name
==========================================================================================
BGP         123        123        21.22.23.25           DOWN            never
0.0.0.0     NA
BGP         123        123        66.66.66.23           DOWN            never
0.0.0.0     CustomerA
BGP         500        500        10.0.0.158             DOWN            never
0.0.0.0     NA
BGP         500        100        10.147.158.2          DOWN            1
0.0.0.0     SENTHIL
BGP         500                                         DOWN            1
0.0.0.0
```

Pseudowire Output

```
#show facility-protocol status
==========================================================================================
Protocols      Peer-IP                VC-ID        VC-Status       VC-Error
==========================================================================================
PWs            10.0.0.146              2            ADMIN DOWN      NA
PWs            10.0.0.146              9            ADMIN DOWN      NA
PWs            10.0.0.146             10           ADMIN DOWN      NA
PWs            10.0.0.146              54           DOWN            NA
PWs            10.0.0.146              87           DOWN            NA
PWs            10.0.0.146              98           DOWN            NA
```

SYncE Output

```
#show facility-protocol status
==========================================================================================
Protocols  Interface                 Mode/QL    QL-IN      QL-Rx-Config   QL-Rx-Overrided

==========================================================================================
SyncE    GigabitEthernet0/1/7        Sync/En    QL-DNU      -                 QL-DNU
SyncE                                Sync/En    QL-DNU      -                 QL-DNU
SyncE                                Sync/En    QL-DNU      -                 QL-DNU
SyncE                                Sync/En    QL-DNU      -                 QL-DNU
```

Bundles Output

```
#show facility-protocol status
==========================================================================================
Protocols         Port-Channel           Bundle-Status      Bundled-Ports       Min-Bundle
==========================================================================================
BUNDLES            Po48                   DOWN                0                   2
```

PTP Output

```
#show facility-protocol status
==========================================================================================
Protocols  Event               Interface              Role     Clock-port-Name    State
       Master-IP
==========================================================================================
PTP CLK_MASTER_PORT_SELECTED   NA                     slave     tomaster            NA
         UNKNOWN

PTP CLK_STATUS_UPDATE     Loopback1588                slave     NA             FREERUN
         NA

PTP CLK_MASTER_PORT_SELECTED   NA                     slave     slave               NA
         21.21.21.21

PTP CLK_STATUS_UPDATE     Loopback0                   slave     NA             ACQUIRING
         NA
```

HSRP Output

```
#show facility-protocol status
=======================================================
Protocols  Interface                Group      State
========================================================
HSRP      HundredGigE0/7/0            1          Init
```

TE Tunnels Output

```
#show facility-protocol status
==========================================================================================
Protocols          Tunnel-Interface            Status
==========================================================================================
MPLS-TE            Tunnel0                     DOWN
MPLS-TE            Tunnel1                     DOWN
```

BFD Output

```
#show facility-protocol status
==========================================================================================
Protocols    Interface                Status          Neigh-Addr     Local-Descriminator
  Interface_index
==========================================================================================
BFD          FortyGigabitEthernet0/8/1   DOWN            NA                  NA
       22
BFD          TenGigabitEthernet0/3/0     DOWN            NA                  NA
       9
BFD          GigabitEthernet0/5/4        DOWN            NA                  NA
       15
BFD          Tunnel1309                  DOWN            NA                  NA
       1601
```

CFM Output

```
#show facility-protocol status
==========================================================================================
Protocols Event          Interface               L-mpid Level Dir BD/VLAN/XCON  ID
Defect-Condition
==========================================================================================
CFM    ENTER_AIS_INT    GigabitEthernet0/0/4     NA     NA    Up   NA            NA  AIS

CFM    ENTER_AIS        GigabitEthernet0/0/4     2      4     Up   XCON          NA  AIS

CFM    ENTER_AIS_INT    GigabitEthernet0/3/6     NA     NA    Up   NA            NA  AIS

CFM    ENTER_AIS        GigabitEthernet0/3/6     2      4     Up   XCON          NA  AIS

==========================================================================================
Protocols Event           R-mpid Level EVC-NAME MA-NAME  Domain  MAC     Status Event-Code
==========================================================================================
CFM    REMOTE_MEP_DOWN          1     NA    SEN_CFM  SEN_CFM  EVC       NA        UP   NA
CFM    REMOTE_MEP_UP            1     NA    SEN_CFM  SEN_CFM  EVC       NA        UP   NA
CFM    CROSSCHECK_MEP_UNKNOWN   1     NA    NA       SEN_CFM  EVC 0022.bdde.05be NA   NA
CFM    CROSS_CONN_SERVICE       1     4     NA       SEN_CFM  EVC 0022.bdde.05be NA   NA
CFM    CONFIG_ERROR             1     NA    NA       SEN_CFM  EVC 0022.bdde.05be NA   NA
```

EVPN PWs Output

```
#show facility-protocol status
==========================================================================================
Protocols          EVPN-ID       Source       Target       Status
==========================================================================================
EVPN-PWs             100           41           30           DOWN
```

Sensory Threshold Violations

```
#show facility-protocol status
===========================================================================================
Protocols PhylIndex SenValue SenType SenScale SenPrecision ThresIndex SenThrValue PhyEntryName
===========================================================================================
SENSOR_THRESH 1211 -103 14 9 1 1 -120 subslot 0/2 transceiver 0 Rx Power Sensor

SENSOR_THRESH 1211 -103 14 9 1 2 -140 subslot 0/2 transceiver 0 Rx Power Sensor

SENSOR_THRESH 1253 -400 14 9 1 3 -310 subslot 0/2 transceiver 3 Rx Power Sensor

SENSOR_THRESH 1253 -400 14 9 1 4 -330 subslot 0/2 transceiver 3 Rx Power Sensor

SENSOR_THRESH 1267 -370 14 9 1 3 -296 subslot 0/2 transceiver 4 Rx Power Sensor

SENSOR_THRESH 1267 -370 14 9 1 4 -310 subslot 0/2 transceiver 4 Rx Power Sensor

SENSOR_THRESH 2001 73 6 9 0 1 0 subslot 0/4 power Sensor 0
```

show facility-protocol status command

To backup the protocols syslog information by capturing the current status of the protocols on the system, use the **show facility-protocol status** command.

Syntax Description

Syntax Description:

There are no keywords.

Command Default

There is no default.

Command Modes

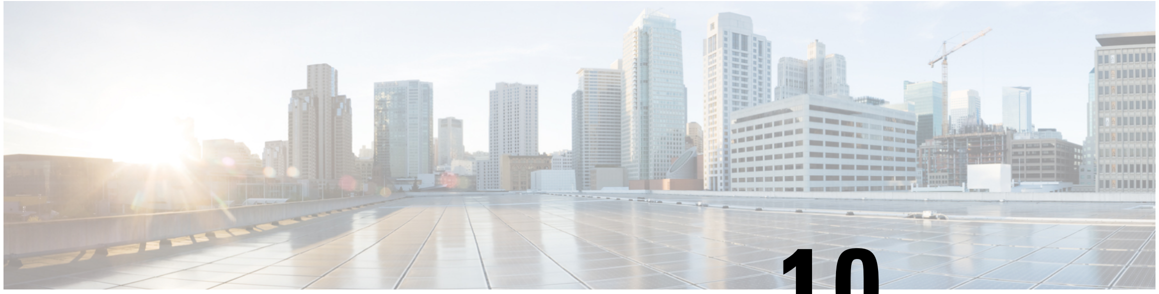
User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.x	Support for this command was introduced on ASR 900, ASR 920, and NCS 4200 Series.

Examples

```
Router# show facility-protocol status
===========================================================================================
Protocols      Peer-IP                VC-ID        VC-Status       VC-Error
===========================================================================================
PWs            10.0.0.146              2            ADMIN DOWN      NA
PWs            10.0.0.146              9            ADMIN DOWN      NA
PWs            10.0.0.146              10           ADMIN DOWN      NA
PWs            10.0.0.146              54           DOWN            NA
PWs            10.0.0.146              87           DOWN            NA
PWs            10.0.0.146              98           DOWN            NA
```



CHAPTER 10

OTN Wrapper Overview

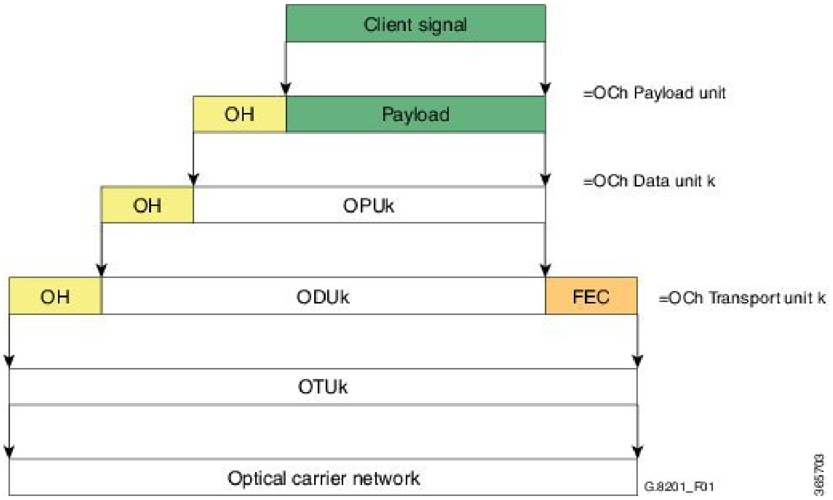
Optical Transport Network (OTN) Wrapper feature provides robust transport services that leverage many of the benefits such as resiliency and performance monitoring, while adding enhanced multi-rate capabilities in support of packet traffic, plus the transparency required by Dense Wavelength Division Multiplexing (DWDM) networks. OTN is the ideal technology to bridge the gap between next generation IP and legacy Time Division Multiplexing (TDM) networks by acting as a converged transport layer for newer packet-based and existing TDM services. OTN is defined in ITU G.709 and allows network operators to converge networks through seamless transport of the numerous types of legacy protocols, while providing the flexibility required to support future client protocols.

OTN Wrapper feature is supported on the following interface modules:

- 8-port 10 Gigabit Ethernet Interface Module (8x10GE) (A900-IMA8Z) (NCS4200-8T-PS) - The encapsulation type is OTU1e and OTU2e.
- 2-port 40 Gigabit Ethernet QSFP Interface Module (2x40GE) (A900-IMA2F) (NCS4200-2Q-P) - The encapsulation type is OTU3.
- 1-port 100 Gigabit Ethernet Interface Module (1X100GE) (NCS4200-1H-PK) (A900-IMA1C) - The encapsulation type is OTU4.

The chassis acts as an aggregator for ethernet, TDM, and SONET traffic to connect to an OTN network and vice versa. The ports on the interface modules are capable of OTN functionality. The OTN controller mode enables the IPoDWDM technology in the interface modules. The OTN Wrapper encapsulates 10G LAN, 40G LAN, and 100G LAN into the corresponding OTU1e or OTU2e, OTU3, and OTU4 containers, respectively. This enables the ports of the interface modules to work in layer 1 optical mode in conformance with standard G.709.

Figure 1: OTN Signal Structure



OTN Frame

The key sections of the OTN frame are the Optical Channel Transport Unit (OTU) overhead section, Optical Channel Data Unit (ODU) overhead section, Optical Channel Payload Unit (OPU) overhead section, OPU payload section, and Forward Error Correction (FEC) overhead section . The network routes these OTN frames across the network in a connection-oriented way. The Overhead carries the information required to identify, control and manage the payload, which maintains the deterministic quality. The Payload is simply the data transported across the network, while the FEC corrects errors when they arrive at the receiver. The number of correctable errors depends on the FEC type.

Advantages of OTN

The following are the advantages of OTN:

- Provides multi-layer performance monitoring and enhanced maintenance capability for signals traversing multi-operator networks.
- Allows Forward Error Correction (FEC) to improve the system performance.
- Provides enhanced alarm handling capability.
- Insulates the network against uncertain service mix by providing transparent native transport of signals encapsulating all client-management information.
- Performs multiplexing for optimum capacity utilization, thereby improving network efficiency.
- Enables network scalability as well as support for dedicated Ethernet services with service definitions.

ODU and OTU

Optical Channel Transport Unit (OTU) and Optical Channel Data Unit (ODU) are the two digital layer networks. All client signals are mapped into the optical channel via the ODU and OTU layer networks.

OTU

The OTU section is composed of two main sections: the Frame Alignment section and the Section Monitoring (SM) section. The OTU Overhead (OH) provides the error detection correction as well as section-layer connection and monitoring functions on the section span. The OTU OH also includes framing bytes, enabling receivers to identify frame boundaries. For more information, see *G.709 document*.

ODU

The ODU section is an internal element allowing mapping or switching between different rates, which is important in allowing operators the ability to understand how the end user pipe is transferred through to the higher network rates. The ODU OH contains path overhead bytes allowing the ability to monitor the performance, fault type and location, generic communication, and six levels of channel protection based on Tandem Connection Monitoring (TCM). For more information, see *G.709 document*.

Deriving OTU1e and OTU2e Rates

A standard OTN frame consists of 255 16-column blocks and the payload rate is 9953280 Kbit/s. This is because the overhead and stuffing in the OTN frames happen at a granularity of 16-column blocks. Thus, OPU payload occupies (3824-16)/16=238 blocks. The ODU occupies 239 blocks and the OTU (including FEC) occupies 255 blocks. Hence, the multiplication factor in the G.709 spec is specified using numbers like 237, 238, 255.

Since OPU2e uses 16 columns that are reserved for stuffing and also for payload, the effective OPU2e frequency is:

- OPU2e = 238/237 x 10312500 Kbit/s = 10.356012 Gbit/s
- ODU2e = 239/237 x 10312500 Kbit/s = 10.399525 Gbit/s
- OTU2e = 255/237 x 10312500 Kbit/s = 11.095727 Gbit/s

Since OPU1e uses 16 columns that are reserved for stuffing and also for payload, the effective OPU1e frequency is:

- OPU1e = 238/238 x 10312500 Kbit/s = 10.3125 Gbit/s
- ODU1e = 239/238 x 10312500 Kbit/s = 10.355829 Gbit/s
- OTU1e = 255/238 x 10312500 Kbit/s = 11.049107 Gbit/s

OTU1e and OTU 2e Support on 8x10GE Interface Module

The OTU1e and OTU2e are mapping mechanisms to map a client 10G Base-R signal to OTN frames transparently as per ITU-T G series Supplement 43 specification. Both these modes are over-clocked OTN modes. These mechanisms provide real bit transparency of 10 GbE LAN signals and are useful for deployment of 10G services.

The OTU1e and OTU2e are inherently intra-domain interfaces (IaDI) and are generally applicable only to a single vendor island within an operator's network to enable the use of unique optical technology. The OTU1e and OTU2e are not standard G.709 bit-rate signals and they do not interwork with the standard mappings of Ethernet using GFP-F. These two over-clocked mechanisms do not interwork with each other. As a result, such signals are only deployed in a point-to-point configuration between equipment that implements the same mapping.

The standard 10 GbE LAN has a data rate of 10.3125 Gbps. In the OTU1e and OTU2e mapping schemes, the full 10.3125 Gbit/s is transported including the 64B/66B coded information, IPG, MAC FCS, preamble, start-of-frame delimiter (SFD) and the ordered sets (to convey fault information). So, the effective OTU2e and OTU1e rates are:

- OTU1e: 11.0491 Gbits/s +/- 100ppm
- OTU2e: 11.0957 Gbits/s +/- 100ppm

The 10GBase-R client signal with fixed stuff bytes is accommodated into an OPU-like signal, then into an ODU-like signal, and further into an OTU-like signal. These signals are denoted as OPU2e, ODU2e and OTU2e, respectively . The OTU1e does not add 16 columns of fixed stuff bytes and hence overall data rate is relatively lesser at 11.0491 Gbps as compared to OTU2e which is 11.0957 Gbps.

The following table shows the standard OTU rates:

Table 12: Standard OTU Rates

G.709 Interface	Line Rate	Corresponding Ethernet Rate	Line Rate
OTU-1e	11.0491 Gbit/s without stuffing bits	10 Gig E-LAN	10.3125 Gbit/s

G.709 Interface	Line Rate	Corresponding Ethernet Rate	Line Rate
OTU-2e	11.0957 Gbit/s without stuffing bits	10 Gig E-LAN	10.3125 Gbit/s
OTU-3	43.018 Gbit/s	STM-256 or OC-768	39.813 Gbit/s

OTU3 Support in 2x40GE Interface Module

When 40GbE LAN is transported over OTN, there is no drop in line rate when the LAN client is mapped into the OPU3 using the standard CBR40G mapping procedure as specified in G.709 clause 17.2.3. The 40G Ethernet signal (41.25 Gbit/s) uses 64B/66B coding making it slightly larger than the OPU3 payload rate that is 40.15 Gbit/s. Hence, to transport 40G Ethernet service over ODU3, the 64B/66B blocks are transcoded into 1024B/1027B block code to reduce their size. The resulting 40.117 Gbit/s transcoded stream is then mapped in standard OPU3.

OTU4 Support on 1-port 100 Gigabit Ethernet Interface Module (1X100GE)

A 100G ethernet client signal running at 103.125 Gbit/s rate can be mapped directly into an OPU4 payload area.

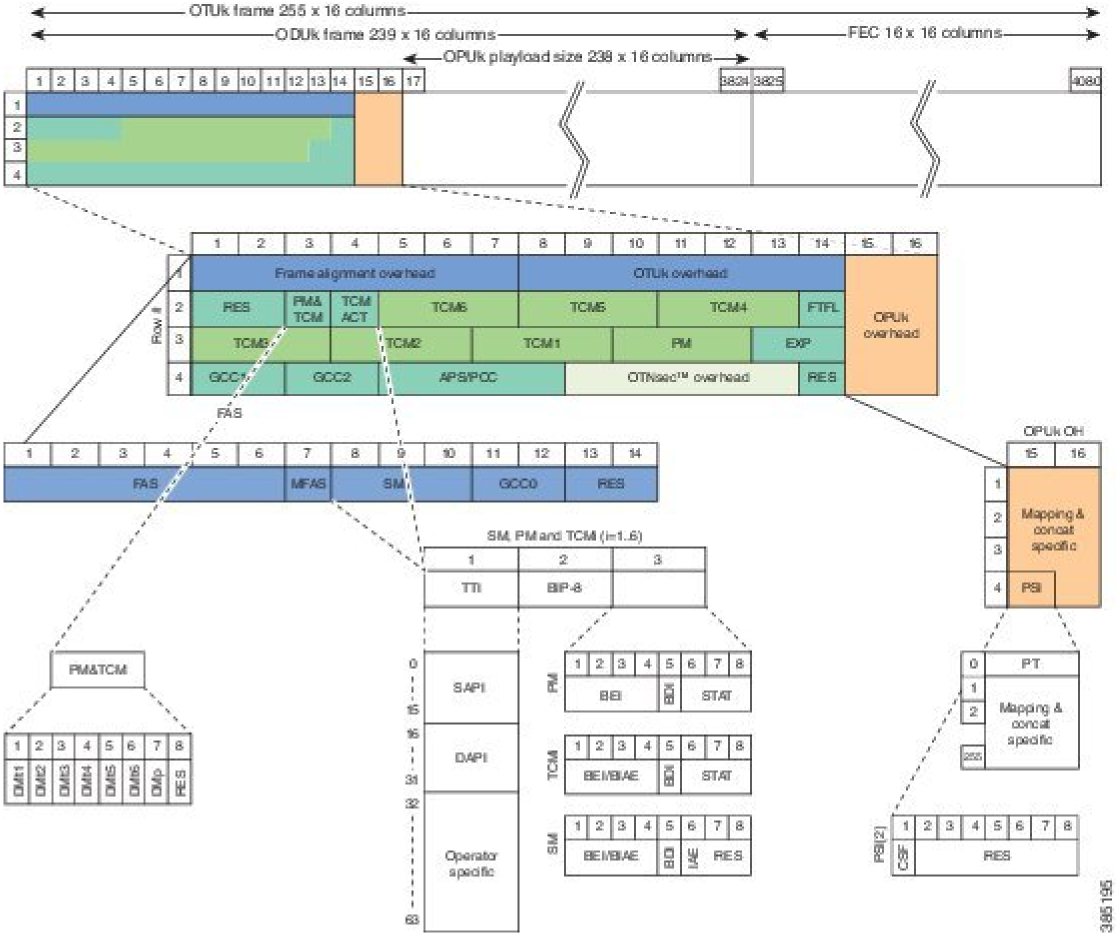
Supported Transceivers

The OTN wrapper feature works with the standard transceiver types that are supported for the LAN mode of 10G, 40G and 100G on the interface modules. The SFP-10G-LR-X, QSFP-40G-LR4, and CPAK-100G-SR10 are used for 8x10GE, 2x40GE, and 1X100GE interface modules, respectively.

OTN Specific Functions

The following figure shows the OTN specific functions related to overhead processing, alarm handling, FEC and TTI:

Figure 2: OTN Specific Functions



Standard MIBS

The following are the standard MIBS:

- RFC2665
- RFC1213
- RFC2907
- RFC2233
- RFC3591

Restrictions for OTN

The following are the restrictions for OTN:

- OTL alarms are not supported.
- FECMISMATCH alarm is not supported.
- Enhanced FEC is not supported.
- Alarm and error counters are visible when the controller is in shutdown state.

DWDM Provisioning

All DWDM provisioning configurations take place on the controller. To configure a DWDM controller, use the controller dwdm command in global configuration mode.

Prerequisites for DWDM Provisioning

The g709 configuration commands can be used only when the controller is in the shutdown state. Use the **no shutdown** command after configuring the parameters, to remove the controller from shutdown state and to enable the controller to move to up state.

Configuring DWDM Provisioning

Use the following commands to configure DWDM provisioning:

```
enable
configure terminal
controller dwdm 0/1/0
```

Configuring Transport Mode in 8x10GE and 2x40GE Interface Modules

Use the **transport-mode** command in interface configuration mode to configure LAN and OTN transport modes in 8x10GE and 2x40GE interface modules. The **transport-mode** command **otn** option has the bit-transparent sub-option, using which bit transparent mapping into OPU1e or OPU2e can be configured.

Use the following commands to configure LAN and OTN transport modes:

```
enable
configure terminal
controller dwdm 0/0/0
transport-mode otn bit-transparent opu1e
```

Note LAN transport mode is the default mode.

To configure the transport administration state on a DWDM port, use the **admin-state** command in DWDM configuration mode. To return the administration state from a DWDM port to the default, use the **no** form of this command.

Verification of LAN Transport Mode Configuration

Use the **show interfaces** command to verify the configuration of LAN transport mode:

```
Router#sh int te0/1/0
TenGigabitEthernet0/1/0 is up, line protocol is up
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 8/255, rxload 193/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 10000Mbps, link type is force-up, media type is SFP-SR
  output flow-control is unsupported, input flow-control is on
  Transport mode LAN
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 04:02:09, output 04:02:09, output hang never
  Last clearing of "show interface" counters 00:29:47
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 7605807000 bits/sec, 14854906 packets/sec
  5 minute output rate 335510000 bits/sec, 655427 packets/sec
     26571883351 packets input, 1700600465344 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     10766634813 packets output, 689064271464 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Verification of OTN Transport Mode Configuration in 8x10GE Interface Modules

Use the **show interfaces** command to verify the configuration of OTN transport mode in 8x10GE interface modules:

```
Router#sh int te0/1/1
TenGigabitEthernet0/1/1 is up, line protocol is up
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 193/255, rxload 7/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 10000Mbps, link type is force-up, media type is SFP-SR
  output flow-control is unsupported, input flow-control is on
  Transport mode OTN (10GBASE-R over OPU1e w/o fixed stuffing, 11.0491Gb/s)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 03:28:14, output 03:28:14, output hang never
  Last clearing of "show interface" counters 00:30:47
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 281326000 bits/sec, 549608 packets/sec
  5 minute output rate 7596663000 bits/sec, 14837094 packets/sec
     10766669034 packets input, 689066159324 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     27457291925 packets output, 1757266795328 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Verification of OTN Transport Mode Configuration in 2x40GE Interface Modules

Use the **show interfaces** command to verify the configuration of OTN transport mode in 2x40GE interface modules:

```
Router#show int  fo0/4/0
FortyGigabitEthernet0/4/0 is up, line protocol is up
  MTU 1500 bytes, BW 40000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 40000Mbps, link type is force-up, media type is QSFP_40GE_SR
  output flow-control is unsupported, input flow-control is on
  Transport mode OTN OTU3 (43.018Gb/s)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  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 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Changing from OTN to LAN Mode

Use the following methods to change from OTN mode to LAN mode:

- Use the following commands to make the transport mode as LAN mode:

```
enable
configure terminal
controller dwdm 0/0/0
transport-mode lan
```

- Use the following commands to set the controller default transport mode as LAN mode:

```
enable
configure terminal
```

```
controller dwdm 0/0/0
default transport-mode
```

Verification of Enabled Ports for Controller Configuration

Use the show controllers command to verify the enables ports for the controller configuration:

```
#show controllers
TenGigabitEthernet0/0/0
TenGigabitEthernet0/0/1
TenGigabitEthernet0/0/2
TenGigabitEthernet0/0/3
TenGigabitEthernet0/0/4
TenGigabitEthernet0/0/5
TenGigabitEthernet0/0/6
TenGigabitEthernet0/0/7
TenGigabitEthernet0/1/0
TenGigabitEthernet0/1/1
FortyGigabitEthernet0/4/0
FortyGigabitEthernet0/4/1
TenGigabitEthernet0/5/0
TenGigabitEthernet0/5/1
TenGigabitEthernet0/5/2
TenGigabitEthernet0/5/3
TenGigabitEthernet0/5/4
TenGigabitEthernet0/5/5
TenGigabitEthernet0/5/6
TenGigabitEthernet0/5/7
#
```

Configuring Transport Mode in 1X100GE Interface Module

Use the **transport-mode** command in interface configuration mode to configure LAN and OTN transport modes in 1X100GE interface module. The **transport-mode** command *otn* option has the bit-transparent sub-option.

Use the following commands to configure LAN and OTN transport modes:

```
enable
configure terminal
controller dwdm 0/0/0
transport-mode otn otu4 100G
```

Note LAN transport mode is the default mode.

To configure the transport administration state on a DWDM port, use the **admin-state** command in DWDM configuration mode. To return the administration state from a DWDM port to the default, use the **no** form of this command.

Verification of Transport Mode Configuration on 1X100GE Interface Module

Use the following commands to verify the transport mode configuration on 1X100GE interface module:

```
#show interfaces Hu0/8/0
HundredGigE0/8/0 is up, line protocol is up
  Hardware is NCS4200-1H-PK, address is 7426.acf6.8048 (bia 7426.acf6.8048)
  MTU 1500 bytes, BW 100000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100000Mbps, link type is force-up, media type is CPAK-100G-SR10
  output flow-control is off, input flow-control is off
  Transport mode OTN OTU4 (111.80997Gb/s)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  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 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out

#

#show controllers dwdm 0/8/0
G709 Information:
Controller dwdm 0/8/0, is up (no shutdown)
Transport mode OTN OTU4
Loopback mode enabled : None
TAS state is : IS
G709 status : Enabled
OTU
        LOS = 0           LOF = 0           LOM = 0
        AIS = 0           BDI = 0           BIP = 0
        TIM = 0           IAE = 0           BEI = 0
ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 0           BEI = 0
FEC Mode: None
Remote FEC Mode: Unknown
        FECM                            = 0
        EC(current second)              = 0
        EC                              = 0
        UC                              = 0
Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI OTU-TIM ODU-AIS ODU-OCI
ODU-LCK ODU-BDI ODU-PTIM ODU-TIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-6
TCA thresholds: SM = 10e-3  PM = 10e-3
OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000
ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000
```

OTN Alarms

OTN supports alarms in each layer of encapsulation. All the alarms follow an alarm hierarchy and the highest level of alarm is asserted and presented as a Syslog message or on the CLI.

OTU Alarms

The types of alarms enabled for reporting:

- AIS - Alarm indication signal (AIS) alarms
- BDI - Backward defect indication (BDI) alarms
- IAE - Incoming alignment error (IAE) alarms
- LOF - Loss of frame (LOF) alarms
- LOM - Loss of multiple frames (LOM) alarms
- LOS - Loss of signal (LOS) alarms
- TIM - Type identifier mismatch (TIM) alarms
- SM - TCA - SM threshold crossing alert
- SD-BER - SM BER is in excess of the SD BER threshold
- SF-BER - SM BER is in excess of the SF BER threshold

ODU Alarms

The types of alarms enabled for reporting:

- AIS - Alarm indication signal (AIS) alarms
- BDI - Backward defect indication (BDI) alarms
- LCK - Upstream connection locked (LCK) error status
- OCI - Open connection indication (OCI) error status
- PM-TCA - Performance monitoring (PM) threshold crossing alert (TCA)
- PTIM - Payload TIM error status

- SD-BER - SM BER is in excess of the SD BER threshold
- SF-BER - SM BER is in excess of the SF BER threshold
- TIM - Type identifier mismatch (TIM) alarms

Configuring OTN Alarm Reports

By default, all the OTN alarm reports are enabled. To control OTN alarm reports, disable all the alarms and enable the specific alarms.

Note You need to shutdown the interface using the **shut** command to configure the alarms.

Configuring OTU Alarm Reports

Use the following commands to configure OTU alarm reports:

```
enable
configure terminal
controller dwdm 0/4/1
shut
g709 otu report bdi
no shut
end
```

Note Fecmismatch is not supported.

Note Use **no g709 otu report** command to disable the OTU alarm reports.

Verification of OTU Alarm Reports Configuration

Use the **show controllers** command to verify OTU alarm reports configuration:

```
#show controllers dwdm 0/4/1
G709 Information:

Controller dwdm 0/4/1, is up (no shutdown)

Transport mode OTN OTU3
Loopback mode enabled : None

TAS state is : IS
G709 status : Enabled
( Alarms and Errors )
OTU
        LOS = 3             LOF = 1             LOM = 0
        AIS = 0             BDI = 0             BIP = 74444
        TIM = 0             IAE = 0             BEI = 37032

ODU
```

```
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 2           BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown
        FECM                           = 0
        EC(current second)             = 0
        EC                             = 186
        UC                             = 10695




Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-6
TCA thresholds: SM = 10e-3  PM = 10e-3

OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000
```

Syslog Generation for LOS Alarm

The following example shows the syslog generation for LOS alarm:

```
(config-if)#
*Jan 16 06:32:50.487 IST: %DWDM-4-G709ALARM: dwdm-0/4/1: LOS declared
*Jan 16 06:32:51.048 IST: %LINK-3-UPDOWN: Interface FortyGigabitEthernet0/4/1, changed state
 to down
*Jan 16 06:32:51.489 IST: %DWDM-4-G709ALARM: dwdm-0/4/1: LOF declared
*Jan 16 06:32:51.495 IST: %DWDM-4-G709ALARM: dwdm-0/4/1: LOS cleared
```

Configuring ODU Alarm Report

Use the following commands to configure ODU alarm reports:

```
enable
configure terminal
controller dwdm 0/4/1
shut
```

```
g709 odu report ais
no shut
end
```

Note Use **no g709 odu report** command to disable the ODU alarm reports.

OTN Threshold

The signal degrade and signal failure thresholds are configured for alerts.

The following types of thresholds are configured for alerts for OTU and ODU layers:

- SD-BER—Section Monitoring (SM) bit error rate (BER) is in excess of the signal degradation (SD) BER threshold.
- SF-BER—SM BER is in excess of the signal failure (SF) BER threshold.
- PM-TCA—Performance monitoring (PM) threshold crossing alert (TCA).
- SM-TCA—SM threshold crossing alert.

Configuring OTU Threshold

To configure OTU threshold:

```
enable
configure terminal
controller dwdm 0/4/1
shut
g709 otu threshold sm-tca 3
no shut
end
```

Note Use **no g709 otu threshold** command to disable OTU threshold.

Configuring ODU Threshold

To configure ODU threshold:

```
enable
configure terminal
controller dwdm 0/4/1
shut
g709 odu threshold sd-ber 3
no shut
end
```

Note Use **no g709 odu threshold** command to disable configuration of ODU threshold.

Verification of OTU and ODU Threshold Configuration

Use the **show controllers** command to verify OTU and ODU threshold configuration:

```
Router#show controllers dwdm 0/1/2
G709 Information:

Controller dwdm 0/1/2, is up (no shutdown)

Transport mode OTN (10GBASE-R over OPU1e w/o fixed stuffing, 11.0491Gb/s)
Loopback mode enabled : None

TAS state is : UNKNWN
G709 status : Enabled

OTU
        LOS = 0           LOF = 0           LOM = 0
        AIS = 0           BDI = 0           BIP = 0
        TIM = 0           IAE = 0           BEI = 0

ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 0           BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown
        FECM                           = 0
        EC(current second)             = 0
        EC                             = 0
        UC                             = 0




Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI OTU-TIM ODU-AIS ODU-OCI
ODU-LCK ODU-BDI ODU-PTIM ODU-TIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-6
TCA thresholds: SM = 10e-3  PM = 10e-3

OTU TTI Sent     String SAPI ASCII      : AABBCCDD
OTU TTI Sent     String DAPI ASCII      : AABBCCDD
OTU TTI Sent     String OPERATOR ASCII  : AABBCCDD
OTU TTI Expected String SAPI ASCII      : AABBCCDD
OTU TTI Expected String DAPI ASCII      : AABBCCDD
OTU TTI Expected String OPERATOR HEX    : AABBCCDD
OTU TTI Received String HEX  : 0052414D45534800000000000000000000052414D455348000
                               0000000000000041414242434344440000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : AABBCCDD
ODU TTI Sent     String DAPI ASCII      : AABBCCDD
ODU TTI Sent     String OPERATOR HEX    : 11223344
ODU TTI Expected String SAPI ASCII      : AABBCCDD
ODU TTI Expected String DAPI ASCII      : AABBCCDD
ODU TTI Expected String OPERATOR HEX    : 11223344
ODU TTI Received String HEX  : 0052414D45534800000000000000000000052414D455348000
                               0000000000000011223344000000000000000000000000000
```

```
                              0000000000000000000000000000000

Router#
```

Configuring OTU Alerts

To configure OTU alerts:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
g709 otu threshold sd-ber
no shutdown
end
```

Configuring ODU Alerts

To configure ODU alerts:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
g709 otu threshold pm-tca
no shutdown
end
```

Configuring ODU Alerts

To configure ODU alerts:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
g709 otu threshold pm-tca
no shutdown
end
```

Verifying Alerts Configuration

Use the show controllers command to verify the alerts configuration:

```
#show controllers dwdm 0/4/1
G709 Information:

Controller dwdm 0/4/1, is down (shutdown)
```

```
Transport mode OTN OTU3
Loopback mode enabled : Line

TAS state is : IS
G709 status : Enabled

OTU
        LOS = 5           LOF = 1           LOM = 0
        AIS = 0           BDI = 0           BIP = 149549
        TIM = 0           IAE = 0           BEI = 74685

ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 2           BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown
        FECM                            = 0
        EC(current second)              = 0
        EC                              = 856
        UC                              = 23165



Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-5
TCA thresholds: SM = 10e-3  PM = 10e-4

OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000
```

Loopback

Loopback provides a means for remotely testing the throughput of an Ethernet port on the router. You can verify the maximum rate of frame transmission with no frame loss. Two types of loopback is supported:

- Internal Loopback - All packets are looped back internally within the router before reaching an external cable. It tests the internal Rx to Tx path and stops the traffic to egress out from the Physical port.
- Line Loopback - Incoming network packets are looped back through the external cable.

Configuring Loopback

To configure loopback:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
loopback line
no shutdown
end
```

Verifying Loopback Configuration

Use the **show controllers** command to verify the loopback configuration:

```
#show controllers dwdm 0/4/1
G709 Information:

Controller dwdm 0/4/1, is up (no shutdown)

Transport mode OTN OTU3
Loopback mode enabled : Line

TAS state is : IS
G709 status : Enabled

OTU
        LOS = 5           LOF = 1           LOM = 0
        AIS = 0           BDI = 0           BIP = 149549
        TIM = 0           IAE = 0           BEI = 74685

ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 2           BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown
        FECM                           = 0
        EC(current second)             = 0
        EC                             = 856
        UC                             = 23165


Detected Alarms: NONE
```

```
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-4
TCA thresholds: SM = 10e-3  PM = 10e-3

OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

#
```

Forward Error Correction

Forward error correction (FEC) is a method of obtaining error control in data transmission in which the source (transmitter) sends redundant data and the destination (receiver) recognizes only the portion of the data that contains no apparent errors. FEC groups source packets into blocks and applies protection to generate a desired number of repair packets. These repair packets may be sent on demand or independently of any receiver feedback.

Standard FEC is supported on 8x10GE and 2x40GE interface modules.

The packets that can be corrected by FEC are known as Error Corrected Packets. The packets that cannot be corrected by FEC due to enhanced bit errors are known as Uncorrected Packets.

Benefits of FEC

The following are the benefits of FEC:

- FEC reduces the number of transmission errors, extends the operating range, and reduces the power requirements for communications systems.
- FEC increases the effective systems throughput.
- FEC supports correction of bit errors occurring due to impairments in the transmission medium.

Configuring FEC

To configure FEC:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 fec standard
no shutdown
end
```

Verifying FEC Configuration

Use the **show controllers** command to verify FEC configuration:

```
G709 Information:

Controller dwdm 0/4/1, is up (no shutdown)

Transport mode OTN OTU3
Loopback mode enabled : Line

TAS state is : IS
G709 status : Enabled

OTU
        LOS = 5           LOF = 1           LOM = 0
        AIS = 0           BDI = 0           BIP = 149549
        TIM = 0           IAE = 0           BEI = 74685

ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 2           BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown <— This is a limitation by which we do not show the remote FEC
mode
        FECM                            = 0
        EC(current second)              = 0
        EC                              = 856       < — This is the counter for Error
corrected bits .
        UC                              = 23165     <- this is the counter for Uncorrected
 alarms .




Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-5
TCA thresholds: SM = 10e-3  PM = 10e-4

OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
```

Trail Trace Identifier

The Trail Trace Identifier (TTI) is a 64-Byte signal that occupies one byte of the frame and is aligned with the OTUk multiframe. It is transmitted four times per multiframe. TTI is defined as a 64-byte string with the following structure:

- TTI [0] contains the Source Access Point Identifier (SAPI) [0] character, which is fixed to all-0s.
- TTI [1] to TTI [15] contain the 15-character source access point identifier (SAPI[1] to SAPI[15]).
- TTI [16] contains the Destination Access Point Identifier (DAPI) [0] character, which is fixed to all-0s.
- TTI [17] to TTI [31] contain the 15-character destination access point identifier (DAPI [1] to DAPI [15]).
- TTI [32] to TTI [63] are operator specific.

TTI Mismatch

TTI mismatch occurs when you have enabled path trace and the "received string" is different from the "expected string". This alarm condition stops traffic.

When TTI mismatch occurs, the interface is brought to down state. This is only supported for SAPI and DAPI and is not supported for **User Operator Data** field.

Configuring TTI

To configure TTI:

```
enable
configure terminal
controller dwdm 0/1/1
shutdown
g709 tti-processing enable
no shutdown
end
```

Trace Identifier Mismatch (TIM) is reported in the Detected Alarms where there is a mismatch in the expected and received string. Action on detection of TIM can be configured in ODU and OTU layers as follows:

```
enable
configure terminal
controller dwdm 0/1/1
shutdown
g709 tti-processing enable otu
```

```
no shutdown
end
```

Configuring TTI for SAPI DAPI Operator Specific Fields

To configure TTI SAPI, DAPI, and operator specific fields for OTU and ODU layers:

```
enable
configure terminal
controller dwdm 0/1/1
g709 fec standard
g709 otu overhead tti sent ascii sapi AABBCCDD
end
```

Verification of TTI SAPI DAPI Operator Specific Fields Configuration

Use the show controller command to verify TTI SAPI, DAPI, Operator Specific fields configuration:

```
Router#show controllers dwdm 0/1/1
G709 Information:
Controller dwdm 0/1/1, is up (no shutdown)

Transport mode OTN (10GBASE-R over OPU1e w/o fixed stuffing, 11.0491Gb/s)

<<truncated other output >>

OTU TTI Sent String SAPI ASCII : AABBCCDD
OTU TTI Sent String DAPI ASCII : AABBCCDD
OTU TTI Sent String OPERATOR ASCII : AABBCCDD
OTU TTI Expected String SAPI ASCII : AABBCCDD
OTU TTI Expected String DAPI ASCII : AABBCCDD
OTU TTI Expected String OPERATOR HEX : AABBCCDD
OTU TTI Received String HEX : 0052414D45534800000000000000000000052414D455348000
0000000000000004141424243434444000000000000000000
000000000000000000000000000000

ODU TTI Sent String SAPI ASCII : AABBCCDD
ODU TTI Sent String DAPI ASCII : AABBCCDD
ODU TTI Sent String OPERATOR HEX : 11223344
ODU TTI Expected String SAPI ASCII : AABBCCDD
```

SNMP Support

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language that is used for monitoring and managing devices in a network.

SNMP sets are not supported for the following tables:

- coiIfControllerTable
- coiOtnNearEndThresholdsTable
- coiOtnFarEndThresholdsTable
- coiFECThresholdsTable

Refer to CISCO-OTN-IF-MIB and *SNMP Configuration Guide* for SNMP support.

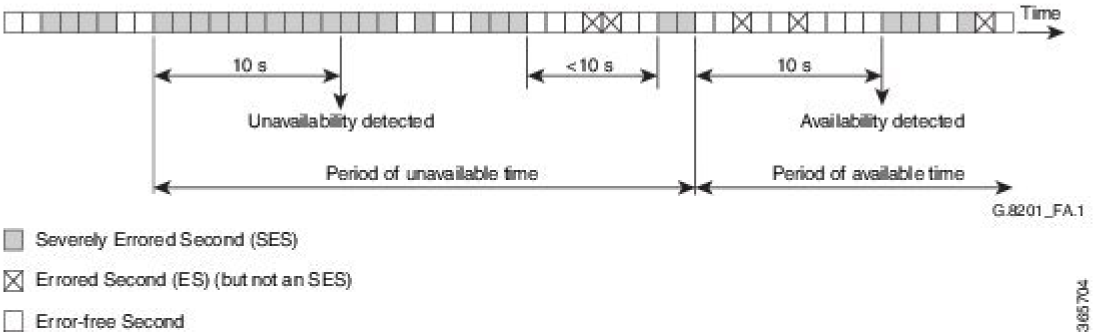
Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for, and report performance data for early detection of problems. Thresholds are used to set error levels for each PM parameter. During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated. The TCAs provide early detection of performance degradation. PM statistics are accumulated on a 15-minute basis, synchronized to the start of each quarter-hour. Historical counts are maintained for 33 15-minutes intervals and 2 daily intervals. PM parameters are collected for OTN and FEC.

Calculation and accumulation of the performance-monitoring data is in 15-minute and 24-hour intervals.

PM parameters require the errored ratio to be less than the standard reference that is dependent on the encapsulation. If any loss or error event does not happen within a second, it is called an error free second. If some error in transmission or alarm happens in a second, the second is called Errored Second. The error is termed as Errored Second or Severely Errored Second or Unavailable Second depending upon the nature of error. The error calculation depends on the Errored Blocks. Errored second is a second where one BIP error or BEI error occurs. Severely Errored Second occurs when the errored frames crosses a threshold or there is an alarm is generated. Unavaliable Second occurs when there are 10 consecutive severely errored seconds.

Figure 3: Performance Monitoring



PM occurs in near end and far end for both encapsulations for ODUk and OTUk. ODU is referred as Path Monitoring (PM) and OTU is referred to as Section Monitoring (SM).

The following table shows the details of each type of PM parameter for OTN:

Table 13: PM Parameters for OTN

Parameter	Definition
BBE-PM	Path Monitoring Background Block Errors (BBE-PM) indicates the number of background block errors recorded in the optical transport network (OTN) path during the PM time interval.
BBE-SM	Section Monitoring Background Block Errors (BBE-SM) indicates the number of background block errors recorded in the OTN section during the PM time interval.

Parameter	Definition
BBER-PM	Path Monitoring Background Block Errors Ratio (BBER-PM) indicates the background block errors ratio recorded in the OTN path during the PM time interval.
BBER-SM	Section Monitoring Background Block Errors Ratio (BBER-SM) indicates the background block errors ratio recorded in the OTN section during the PM time interval.
ES-PM	Path Monitoring Errored Seconds (ES-PM) indicates the errored seconds recorded in the OTN path during the PM time interval.
ESR-PM	Path Monitoring Errored Seconds Ratio (ESR-PM) indicates the errored seconds ratio recorded in the OTN path during the PM time interval.
ESR-SM	Section Monitoring Errored Seconds Ratio (ESR-SM) indicates the errored seconds ratio recorded in the OTN section during the PM time interval.
ES-SM	Section Monitoring Errored Seconds (ES-SM) indicates the errored seconds recorded in the OTN section during the PM time interval.
FC-PM	Path Monitoring Failure Counts (FC-PM) indicates the failure counts recorded in the OTN path during the PM time interval.
FC-SM	Section Monitoring Failure Counts (FC-SM) indicates the failure counts recorded in the OTN section during the PM time interval.
SES-PM	Path Monitoring Severely Errored Seconds (SES-PM) indicates the severely errored seconds recorded in the OTN path during the PM time interval.
SES-SM	Section Monitoring Severely Errored Seconds (SES-SM) indicates the severely errored seconds recorded in the OTN section during the PM time interval.
SESR-PM	Path Monitoring Severely Errored Seconds Ratio (SESR-PM) indicates the severely errored seconds ratio recorded in the OTN path during the PM time interval.

Parameter	Definition
SESR-SM	Section Monitoring Severely Errored Seconds Ratio (SESR-SM) indicates the severely errored seconds ratio recorded in the OTN section during the PM time interval.
UAS-PM	Path Monitoring Unavailable Seconds (UAS-PM) indicates the unavailable seconds recorded in the OTN path during the PM time interval.
UAS-SM	Section Monitoring Unavailable Seconds (UAS-SM) indicates the unavailable seconds recorded in the OTN section during the PM time interval.

The following table shows the details of each type of PM parameter for FEC:

Table 14: PM Parameters for FEC

Parameter	Definition
EC	Bit Errors Corrected (BIEC) indicated the number of bit errors corrected in the DWDM trunk line during the PM time interval.
UC-WORDS	Uncorrectable Words (UC-WORDS) is the number of uncorrectable words detected in the DWDM trunk line during the PM time interval.

OTUk Section Monitoring

Section Monitoring (SM) overhead for OTUk is terminated as follows:

- TTI
- BIP
- BEI
- BDI
- IAE
- BIAE

BIP and BEI counters are block error counters (block size equal to OTUk frame size). The counters can be read periodically by a PM thread to derive one second performance counts. They are sufficiently wide for software to identify a wrap-around with up to 1.5 sec between successive readings.

The following OTUk level defects are detected:

- dAIS
- dTIM
- dBDI

- dIAE
- dBIAE

Status of the defects is available through CPU readable registers, and a change of status of dLOF, dLOM, and dAIS will generate an interruption.

ODUk Path Monitoring

Path Monitoring (PM) overhead for higher order ODUk and lower order ODUk is processed as follows:

- TTI
- BIP
- BEI
- BDI
- STAT including ODU LCK/OCI/AIS

The following ODUk defects are detected:

- dTIM
- dLCK and dAIS (from STAT field)
- dBDI

LOS, OTU LOF, OOF and ODU-AIS alarms bring down the interface in system.

Configuring PM Parameters for FEC

To set TCA report status on FEC layer in 15-minute interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 15-min fec report ec-bits enable
pm 15-min fec report uc-words enable
end
```

To set TCA report status on FEC layer in 24-hour interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 24-hr fec report ec-bits enable
pm 24-hr fec report uc-words enable
end
```

To set threshold on FEC layer in 15-minute interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 15-min fec threshold ec-bits
pm 15-min fec threshold uc-words
end
```

To set threshold on FEC layer in 24-hour interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 24-hr fec threshold ec-bits
pm 24-hr fec threshold uc-words
end
```

Configuring PM Parameters for OTN

To set OTN report status in 15-minute interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 15-min otn report es-pm-ne enable
end
```

To set OTN report status in 24-hour interval:

```
enable
configure terminal
controller dwdm slot/bay/port
pm 24-hr otn report es-pm-ne enable
end
```

To set OTN threshold in 15-minute interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 15-min otn threshold es-pm-ne
end
```

To set OTN threshold in 24-hour interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 24-hr otn threshold es-pm-ne
end
```

Verifying PM Parameters Configuration

Use the **show controllers** command to verify PM parameters configuration for FEC in 15-minute interval:

```
Router#show controllers dwdm 0/1/0 pm interval 15-min fec 0
g709 FEC in the current interval [9 :15:00 - 09:16:40 Thu Jun 9 2016]

FEC current bucket type : INVALID
    EC-BITS   :            0    Threshold :          200   TCA(enable)  : YES
    UC-WORDS  :            0    Threshold :           23  TCA(enable)  : YES


Router#show controllers dwdm 0/1/0 pm interval 15-min fec 1
g709 FEC in interval 1 [9 :00:00 - 9 :15:00 Thu Jun 9 2016]

FEC current bucket type : VALID
    EC-BITS   :            0      UC-WORDS  :            0
```

Use the **show controllers** command to verify PM parameters configuration for FEC in 24-hour interval:

```
Router#show controllers dwdm 0/1/0 pm interval 24 fec 0
g709 FEC in the current interval [00:00:00 - 09:17:01 Thu Jun 9 2016]

FEC current bucket type : INVALID
    EC-BITS   :            0    Threshold :            0   TCA(enable)  : NO
    UC-WORDS  :            0    Threshold :            0  TCA(enable)  : NO


Router#show controllers dwdm 0/1/0 pm interval 24 fec 1
g709 FEC in interval 1 [00:00:00 - 24:00:00 Wed Jun 8 2016]

FEC current bucket type : VALID
    EC-BITS   :          717      UC-WORDS  :      1188574
```

Use the **show controllers** command to verify PM parameters configuration for OTN in 15-minute interval:

```
Router#show controllers dwdm 0/1/0 pm interval 15-min otn 0
g709 OTN in the current interval [9 :15:00 - 09:15:51 Thu Jun 9 2016]

OTN current bucket type: INVALID

OTN Near-End Valid : YES
    ES-SM-NE    :        0     Threshold :        0   TCA(enable)  : NO
    ESR-SM-NE   :  0.00000     Threshold :  0.00010   TCA(enable)  : YES
    SES-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    SESR-SM-NE  :  0.00000     Threshold :  0.02300   TCA(enable)  : NO
    UAS-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBE-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBER-SM-NE  :  0.00000     Threshold :  0.02300   TCA(enable)  : NO
    FC-SM-NE    :        0     Threshold :        0   TCA(enable)  : NO
    ES-PM-NE    :        0     Threshold :      200   TCA(enable)  : YES
    ESR-PM-NE   :  0.00000     Threshold :  1.00000   TCA(enable)  : NO
    SES-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    SESR-PM-NE  :  0.00000     Threshold :  0.02300   TCA(enable)  : NO
    UAS-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBE-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBER-PM-NE  :  0.00000     Threshold :  0.02300   TCA(enable)  : NO
    FC-PM-NE    :        0     Threshold :        0   TCA(enable)  : NO


OTN Far-End Valid : YES
    ES-SM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ESR-SM-FE   :  0.00000       Threshold :  1.00000   TCA(enable)  : NO
    SES-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    SESR-SM-FE  :  0.00000       Threshold :  0.02300   TCA(enable)  : NO
    UAS-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBE-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBER-SM-FE  :  0.00000       Threshold :  0.02300   TCA(enable)  : NO
    FC-SM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ES-PM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ESR-PM-FE   :  0.00000       Threshold :  1.00000   TCA(enable)  : NO
    SES-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    SESR-PM-FE  :  0.00000       Threshold :  0.02300   TCA(enable)  : NO
    UAS-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBE-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBER-PM-FE  :  0.00000       Threshold :  0.02300   TCA(enable)  : NO
    FC-PM-FE    :        0       Threshold :        0   TCA(enable)  : NO


Router#show controllers dwdm 0/1/0 pm interval 15-min otn 1
g709 OTN in interval 1 [9 :00:00 - 9 :15:00 Thu Jun 9 2016]

OTN current bucket type: VALID
OTN Near-End Valid : YES        OTN Far-End Valid : YES
    ES-SM-NE    :        0         ES-SM-FE    :        0
    ESR-SM-NE   :  0.00000         ESR-SM-FE   :  0.00000
    SES-SM-NE   :        0         SES-SM-FE   :        0
    SESR-SM-NE  :  0.00000         SESR-SM-FE  :  0.00000
    UAS-SM-NE   :        0         UAS-SM-FE   :        0
    BBE-SM-NE   :        0         BBE-SM-FE   :        0
    BBER-SM-NE  :  0.00000         BBER-SM-FE  :  0.00000
    FC-SM-NE    :        0         FC-SM-FE    :        0
    ES-PM-NE    :        0         ES-PM-FE    :        0
    ESR-PM-NE   :  0.00000         ESR-PM-FE   :  0.00000
    SES-PM-NE   :        0         SES-PM-FE   :        0
    SESR-PM-NE  :  0.00000         SESR-PM-FE  :  0.00000
    UAS-PM-NE   :        0         UAS-PM-FE   :        0
    BBE-PM-NE   :        0         BBE-PM-FE   :        0
    BBER-PM-NE  :  0.00000         BBER-PM-FE  :  0.00000
    FC-PM-NE    :        0         FC-PM-FE    :        0
```

Use the **show controllers** command to verify PM parameters configuration for OTN in 24-hour interval:

```
Router#show controllers dwdm 0/1/0 pm interval 24-hour otn 0
g709 OTN in the current interval [00:00:00 - 09:16:10 Thu Jun 9 2016]

OTN current bucket type: INVALID

OTN Near-End Valid : YES
    ES-SM-NE    :        0     Threshold :        0   TCA(enable)  : NO
    ESR-SM-NE   :  0.00000     Threshold :  0.00000   TCA(enable)  : NO
    SES-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    SESR-SM-NE  :  0.00000     Threshold :  0.00000   TCA(enable)  : NO
    UAS-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBE-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBER-SM-NE  :  0.00000     Threshold :  0.00000   TCA(enable)  : NO
    FC-SM-NE    :        0     Threshold :        0   TCA(enable)  : NO
    ES-PM-NE    :        0     Threshold :        0   TCA(enable)  : NO
    ESR-PM-NE   :  0.00000     Threshold :  0.00000   TCA(enable)  : NO
    SES-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    SESR-PM-NE  :  0.00000     Threshold :  0.00000   TCA(enable)  : NO
    UAS-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBE-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBER-PM-NE  :  0.00000     Threshold :  0.00000   TCA(enable)  : NO
    FC-PM-NE    :        0     Threshold :        0   TCA(enable)  : NO


OTN Far-End Valid : YES
    ES-SM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ESR-SM-FE   :  0.00000       Threshold :  0.00000   TCA(enable)  : NO
    SES-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    SESR-SM-FE  :  0.00000       Threshold :  0.00000   TCA(enable)  : NO
    UAS-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBE-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBER-SM-FE  :  0.00000       Threshold :  0.00000   TCA(enable)  : NO
    FC-SM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ES-PM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ESR-PM-FE   :  0.00000       Threshold :  0.00000   TCA(enable)  : NO
    SES-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    SESR-PM-FE  :  0.00000       Threshold :  0.00000   TCA(enable)  : NO
    UAS-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBE-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBER-PM-FE  :  0.00000       Threshold :  0.00000   TCA(enable)  : NO
    FC-PM-FE    :        0       Threshold :        0   TCA(enable)  : NO
```

```
Router#show controllers dwdm 0/1/0 pm interval 24-hour otn 1
g709 OTN in interval 1 [00:00:00 - 24:00:00 Wed Jun 8 2016]

OTN current bucket type: INVALID

OTN Near-End Valid : YES        OTN Far-End Valid : NO
    ES-SM-NE    :        7         ES-SM-FE    :        0
    ESR-SM-NE   :  0.00000         ESR-SM-FE   :  0.00000
    SES-SM-NE   :        7         SES-SM-FE   :        0
    SESR-SM-NE  :  0.00000         SESR-SM-FE  :  0.00000
    UAS-SM-NE   :       41         UAS-SM-FE   :        0
    BBE-SM-NE   :        0         BBE-SM-FE   :        0
    BBER-SM-NE  :  0.00000         BBER-SM-FE  :  0.00000
    FC-SM-NE    :        3         FC-SM-FE    :        0
    ES-PM-NE    :        2         ES-PM-FE    :        1
    ESR-PM-NE   :  0.00000         ESR-PM-FE   :  0.00000
    SES-PM-NE   :        0         SES-PM-FE   :        0
    SESR-PM-NE  :  0.00000         SESR-PM-FE  :  0.00000
    UAS-PM-NE   :        0         UAS-PM-FE   :        0
    BBE-PM-NE   :        3         BBE-PM-FE   :        1
    BBER-PM-NE  :  0.00000         BBER-PM-FE  :  0.00000
    FC-PM-NE    :        0         FC-PM-FE    :        0
```

If TCA is enabled for OTN or FEC alarm, a syslog message is displayed for the 15-minute or 24-hour interval as follows:

```
*Jun  9 09:18:02.274: %PMDWDM-4-TCA: dwdm-0/1/0: G709 ESR-SM NE value (540) threshold (10)
 15-min
```

Troubleshooting Scenarios

The following table shows the troubleshooting solutions for the feature.

Problem	Solution
Link is not coming up	Perform shut and no shut actions of the interface. Check for TTI Mismatch. Verify the major alarms. Verify the FEC mode. Verify that Cisco supported transreceiver list is only used on both sides .
Incrementing BIP Error	Verify FEC Mismatch.
FEC contains UC and EC errors and link is not coming up	Verify the FEC Mismatch.

Associated Commands

The following commands are used to configure OTN Wrapper:

Commands	Links
controller dwdm	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp1680149833
g709 disable	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp7175256270
g709 fec	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3986227580
g709 odu report	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3893551740
g709 odu threshold	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3365653610
g709 otu report	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3306168000
g709 otu threshold	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp2500217585
g709 overhead	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp6997702360
g709 tti processing	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3679037909
pm fec threshold	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp8624772760
pm otn report	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp2518071708
pm otn threshold	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp1512678519
show controller dwdm	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s2.html#wp7346292950

Commands	Links
show interfaces	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s4.html#wp2987586133
transport-mode	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-t1.html#wp3012872075

CHAPTER 11

Configuring 1G Traffic on 8-port 10 Gigabit Ethernet Interface Module

The 8-port 10 Gigabit Ethernet Interface Module (8X10GE) has eight ports and is supported on the RSP3 module. Prior to Cisco IOS XE Everest 16.5.1, 1G traffic support was provided only with the devices placed in the access layer. Effective Cisco IOS XE Everest 16.5.1, 1G traffic support is provided to devices in the distribution layer. Thus, all the eight port provide support for 1G mode as well as 10G mode.

The configuration of 1G traffic on 8X10GE interface module provides cost-effective solution during migration from 1G mode to 10G mode as a single device supports both the modes.

Note By default, the 8X10GE inteface module comes up in the 10G mode after reboot.

Restrictions for 1G Mode on 8X10 GE Interface Module

- SFP+ is not supported on 1G mode, but the physical link with SFP+ in 1G mode comes up.
- Support of 1G mode on a port and 10G mode on another port in the same interface module is not supported.
- Precision Time Protocol (PTP) is not supported.
- Sync-E is not supported. However, Sync-E is supported in over subscription mode on the interface module.
- Port channel bundling on 1G mode is not supported.
- Although 1G mode is supported on the interface module, the interface is displayed as "Te0/X/Y" depending on the port numbers for both 1G and 10G modes.

- 10G mode support on 8X10GE interface module does not change with dual-rate support.
- Carrier delay configuration of less than 2 seconds is not supported on both 1G and 10G modes for the 8-port 10 Gigabit Ethernet interface module.

Configuring 1G Mode

Defaulting the Interface Module:

```
enable
hw-module subslot 0/4 default
end
```

Changing the Mode:

```
enable
configure terminal
hw-module subslot 0/4 ether-mode 1G
end
```

Configuring the Ports:

```
enable
configure terminal
interface te0/4/0
ip address 63.0.0.1 255.0.0.0
end
```

Verifying 1G Mode Configuration

The transport mode is LAN (1GB/s). The speed and bandwidth are 1000 Mbps and 1000000 Kbit/sec, respectively.

To verify the configuration, use **show interface** command in privileged EXEC mode:

```
Router#show interface tengigabitethernet0/4/0

   TenGigabitEthernet0/4/0 is up, line protocol is up
   Hardware is A900-IMA8Z, address is c8f9.f98d.2024 (bia c8f9.f98d.2024)
   Internet address is 50.0.0.1/8
   MTU 1500 bytes, te0/4/0, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   Full Duplex, 1000Mbps, link type is auto, media type is SX
   output flow-control is off, input flow-control is off
   Transport mode LAN (1Gb/s)
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input 00:08:24, output 00:08:24, output hang never
   Last clearing of "show interface" counters 00:07:59
   Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: fifo
  …..
```

To verify the slots configured in 1G mode, use the **show running-config | i ether-mode** command in privileged EXEC mode:

```
Router#show running-config | i ether-mode
hw-module subslot 0/3 ether-mode 1g
```

```
hw-module subslot 0/4 ether-mode 1g
hw-module subslot 0/11 ether-mode 1g
```

To verify the bandwidth and port speed, use the **show platform hardware pp active interface all** in privileged EXEC mode:

```
Router#show platform hardware pp active interface all
      Interface manager platform keys
     -------------------------------------------------

     Name: TenGigabitEthernet0/4/7, Asic: 0, hwidx: 9
     lpn: 0, ppn: 9, gid: 9, mac: c8f9.f98d.202b
    InLportId: 0, ELportId: 0, dpidx: 31, l3ID: 25
    port_flags: 0, port_speed: 1000 Mbps, efp_count: 0, destIndex: 9, intType: 1
    etherchnl: 0, efp: 0, bdi: 0, l2PhyIf: 0, l3PhyIf: 1, l3TDM: 0, loopBack: 0
    tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
    bandwidth: 1000000, fcid: 0, cid: 0, mpls_tbid: 0, protocols: 4
    v4_netsmask: 8, v4_tableid: 8, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
   bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
   vrfid: 8, enctype: 0, admin_state: 1, admin_state_oir: 0

   Name: TenGigabitEthernet0/4/6, Asic: 0, hwidx: 10
   lpn: 0, ppn: 10, gid: 10, mac: c8f9.f98d.202a
   InLportId: 0, ELportId: 0, dpidx: 30, l3ID: 24
   port_flags: 0, port_speed: 1000 Mbps, efp_count: 0, destIndex: 10, intType: 1
  etherchnl: 0, efp: 0, bdi: 0, l2PhyIf: 0, l3PhyIf: 1, l3TDM: 0, loopBack: 0
  tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
  bandwidth: 1000000, fcid: 0, cid: 0, mpls_tbid: 0, protocols: 4
  v4_netsmask: 8, v4_tableid: 6, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
  bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
  vrfid: 6, enctype: 0, admin_state: 1, admin_state_oir: 0
```

Configuring 10G Mode from 1G Mode

Deafulting the Interface Module:

```
enable
hw-module subslot 0/4 default
end
```

Changing the Mode:

```
enable
configure terminal
hw-module subslot 0/4 ether-mode 10G
end
```

Note The default is 10G mode.

Configuring the Ports:

```
enable
configure terminal
interface te0/4/0
ip address 63.0.0.1 255.0.0.0
end
```

Verifying 10G Mode Configuration

To verify the configuration, use **show interface** command in privileged EXEC mode:

```
Router#show interface tengigabitethernet0/4/0
   TenGigabitEthernet0/4/0 is up, line protocol is up
   Hardware is A900-IMA8Z, address is c8f9.f98d.2024 (bia c8f9.f98d.2024)
   Internet address is 50.0.0.1/8
   MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   Full Duplex, 10000Mbps, link type is auto, media type is SX
   output flow-control is off, input flow-control is off
   Transport mode LAN
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input 00:08:24, output 00:08:24, output hang never
   Last clearing of "show interface" counters 00:07:59
   Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: fifo
  …..
```

Note For 10G mode, the **hw-module subslot 0/x ether-mode 10G** command is not displayed when you use **show running-config** command.

To verify the bandwidth and port speed, use the **show platform hardware pp active interface all** in privileged EXEC mode:

```
Router#show platform hardware pp active interface all
      Interface manager platform keys
     -------------------------------------------------

     Name: TenGigabitEthernet0/4/7, Asic: 0, hwidx: 9
     lpn: 0, ppn: 9, gid: 9, mac: c8f9.f98d.202b
    InLportId: 0, ELportId: 0, dpidx: 31, l3ID: 25
    port_flags: 0, port_speed: 10000 Mbps, efp_count: 0, destIndex: 9, intType: 1
    etherchnl: 0, efp: 0, bdi: 0, l2PhyIf: 0, l3PhyIf: 1, l3TDM: 0, loopBack: 0
    tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
    bandwidth: 10000000, fcid: 0, cid: 0, mpls_tbid: 0, protocols: 4
    v4_netsmask: 8, v4_tableid: 8, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
   bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
   vrfid: 8, enctype: 0, admin_state: 1, admin_state_oir: 0

   Name: TenGigabitEthernet0/4/6, Asic: 0, hwidx: 10
   lpn: 0, ppn: 10, gid: 10, mac: c8f9.f98d.202a
   InLportId: 0, ELportId: 0, dpidx: 30, l3ID: 24
   port_flags: 0, port_speed: 10000 Mbps, efp_count: 0, destIndex: 10, intType: 1
  etherchnl: 0, efp: 0, bdi: 0, l2PhyIf: 0, l3PhyIf: 1, l3TDM: 0, loopBack: 0
  tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
  bandwidth: 10000000, fcid: 0, cid: 0, mpls_tbid: 0, protocols: 4
  v4_netsmask: 8, v4_tableid: 6, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
  bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
  vrfid: 6, enctype: 0, admin_state: 1, admin_state_oir: 0
```

Associated Commands

The following commands are used to configure 8-port 10 Gigabit Ethernet Interface Module (8X10GE):

Commands	Links
hw-module subslot	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp4618355370
show platform hardware pp active interface all	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s5.html

Overview of Over Subscription and Partial Port Modes on the 8-port 10 Gigabit Ethernet Interface Module

The 8-port 10 Gigbait Ethernet interface module (8X10GE) reqiures eight backplane XFI lines to the ASIC to operate efficiently. The chassis has different backplance capcity or bandwidth on each of its subslot. The 8X10GE interface module could only be used in sublsots that offered the eight XFI backplance lines. The following table shows the slots that 8X10GE interface module support without over subscription mode:

Slot No	Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9	Slot 10	Slot 11	Slot 12	Slot 13	Slot 14	Slot 15
8X10GE	No	No	No	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No	No

Note The router supports the 8X10GE interface module individually on the above slots, and offer eight XFI/SFI lines. But as a combination of slots to support 400G bandwidth, only five slots are supported for the 8X10GE interface module. With over subscription or partial mode enabled on the router six slots are available to support the bandwidth.

Over subscription mode enables the operation of the 8X10GE interface module in all subslots with a lesser backplane capacity. Hence, with over subscription mode enabled, all the front plane ports of the interface module are able to receive and transmit traffic.

Partial port mode is used to free the used serializer/deserializer (SerDes) lines to accommodate interface modules that support over subscription in those slots that may utilize the shared SerDes. The advantage of this mode is that the Channelized Network Interface Scheduler (CNIS) of ASIC, a limited resource, is not utilized, as compared to the over subscription mode.

Both these modes aid in increasing the nmber of interface modules in the maximum number of subslots on the chassis.

Over Subscription Mode

Over subscription mode is introduced to support population of maximum number of interface modules on the chassis.

The 8X10GE interface module requires eight backplane XFI lines to operate, where each front plane port fully utilizes a backplane XFI line. Hence, it operates with an overall bandwidth of 80Gbps. When over subscription is enabled, a group of front plane ports are channelized onto a single backplane XFI line, which reduces the bandwidth based on the number of ports multiplexed onto the backplane XFI line.

When the 8X10GE interface module is in over subscribed mode, all the eight front plane ports are functional.

2:1 — Two front plane ports are multiplexed onto one backplane XFI. The overall bandwidth of the interface module is 40Gbps.

Partial Port Mode

Partial port mode is also introduced to support maximum number of interface modules on the chassis.

This mode, unlike over subscription mode does not multiplex the front plane port, but blocks some front plane ports to free up the backplane XFI lines used by them.

Partial Port mode has one variant:

4 port mode — Only four front plane ports are enabled. Each port uses one backplane XFI line. Hence each port supports 10Gbps data rate, and the interface module supports 40Gbps datarate.

Prerequisites for Over Subscription Mode on the 8-port 10 Gigabit Ethernet Interface Module

- FPGA must be upgraded to version 0.22. Use the **upgrade hw-module subslot 0/x fpd bundled reload** command to upgrade manually, before configuring over-subscription mode.

Restrictions for Over Subscription Mode 8-port 10 Gigabit Ethernet Interface Module

The following restrictions are applicable for the over subscription mode on the 8-port 10 Gigabit Ethernet Interface Module (A900-IMA8Z) on the ASR 907 Router:

- Traffic prioritization is supported, but policing is not supported.
- PTP over over subscription mode is not supported.
- Dynamic over subscription mode change does not work. Reload the router after any mode change.

Supported Features and Constraints

Following are the supported features and constraints for configuring over subscription and partial port mode on the 8X10 GE interface module.

Table 15: Over Subscription Mode and Partial Port Mode Support Features and Constraints

	8X10 GE Over Subscription Mode	**4 X10 G Partial Port Mode**
Supported Platforms	ASR 907 RSP3-400	ASR 907 RSP3-400
FPGA Mode	Supported only with XFI passthrough mode Minimum version 0.22	Supported on both XFI passthrough and port expansion mode

	8X10 GE Over Subscription Mode	4 X10 G Partial Port Mode
Subslots	Supported on only selected subslots	Supported on only selected subslots
Mode Enablement	Activated on router reload	Activated on router reload
Backplane SerDes Selection	Static; Cannot define backplane SerDes	Static; Cannot define backplane SerDes
Dual Rate Support (1G / 10G)	Not supported on 1G mode in Cisco IOS XE Fuji 16.9.1.	Not supported on 1G mode in Cisco IOS XE Fuji 16.9.1.
LAN/WAN/OTN Support	10G Eth (LAN) mode is supported in Cisco IOS XE Fuji 16.9.1.	Supports LAN/WAN/OTN modes

Supported Subslots

The table shows the subslots of the different over subscription modes and also provides information about the SerDes line from the ASIC (multiplexed) to the frontplane ports on the chassis:

Table 16: Supported Subslots and SerDes Lines used by the 8X10GE Interface Module with Over Subscription Modes

Mode	Supported Slots	SerDes Lines Used	Enabled Ports
2:1 over subscription mode	3, 4	2, 3 6, 7	All ports
	11, 12	0, 1,2, 3	
4 Port Mode (Partial Port mode)	3,4	2,3,6,7	0,1,4,5

Note Serializer/Deserializer (SerDes) is not released when dependant slot interface modules are in shutdown unpowered state.

FPGA Operating Mode

The FPGA operates in the following modes. The FPGA operating modes are selected by configuration.

- Port Expansion Mode — Allows port expansion on QSGMII based interface module such as the 8X1G interface module or 8x1G+10G combo interface module. The FPGA consumes the port expansion quad on ASIC.
- XFI Passthrough Mode — Supports XFI passthrough for enabling new XFI lines in certain slots of the chassis.

Note System reload is required after changing the FPGA mode .

Note Over subscription on the 8X10GE interface module is supported only with the XFI Passthrough mode.

The **license feature service-offlload enable** command is used to change the FPGA mode to the XFI Passsthrough mode.

The default setting of this command is the **no** form of the command. The default FPGA operation mode is XLAUI-QSGMII Port expansion mode.

Maximum Slot Population of the 8-port 10 Gigabit Ethernet Interface Module

Over subscription and partial port mode is implemented to free up the shared SerDes lines to other interface modules, and to also populate the 8X10GE interface modules in maximum possible slots with an optimum bandwidth support.

Note A total of six 8x10GE interface modules are populated on the ASR 907 chassis with the RSP3-400 module.

The following table shows the modes selected on each subslot, and the CNIS utilized in that subslot in order to realise the maximum slot population of 8X10GE interface module.

Table 17: Maximum Slot Population of the 8X10 GE Interface Module

Subslot	8X10 GE Interface Module Mode	Port Numbers	SerDes Numbers	ASIC No.	CNIS Used
4	4X10G Partial Port	0	27	ASIC-1	0
		1	26		
		4	15		
		5	14		
8	8X10G Fully Subscibed Mode	0	7	ASIC-1	0
		1	6		
		2	5		
		3	4		
		4	3		
		5	2		
		6	1		
		7	0		

Subslot	8X10 GE Interface Module Mode	Port Numbers	SerDes Numbers	ASIC No.	CNIS Used
12	4X10G Partial Port	4	11	ASIC-1	0
		5	10		
		6	9		
		7	8		
3	4X10G Partial Port	0	27	ASIC-0	0
		1	26		
		4	15		
		5	14		
7	8X10G Fully Subscribed	0	7	ASIC-0	0
		1	6		
		2	5		
		3	4		
		4	3		
		5	2		
		6	1		
		7	0		
11	4X10G Partial Port	4	11	ASIC-0	0
		5	10		
		6	9		
		7	8		

Configuring Over Subscription and Partial Mode

Use the **platform hw-module configuration** to configure the mode on the chassis.

- Example: Configuring over subscription mode

```
Router(config)#platform hw-module configuration
```

```
Router(conf-plat-hw-conf)# hw-module 0/12 A900-IMA8Z mode 8x10G-2:1-OS
```

- Example: Confguring parital port mode

```
Example: Router(config)#platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/3 A900-IMA8Z mode 4-ports-only
```

Persistent Bandwidth for A900-IMA8Z

Table 18: Feature History

Feature Name	Release Information	Description
Persistent Bandwidth for 8-port 10 Gigabit Ethernet Interface module (A900-IMA8Z)	Cisco IOS XE Cupertino 17.9.1	This feature persistently retains the configured bandwidth value of the interface for 8-port 10 Gigabit Ethernet Interface module (A900-IMA8Z) across triggers such as interface shut or no-shut, IM reload, Stateful Switchover (SSO), and so on. This feature is only supported on Cisco RSP3 module. This feature is only supported on NCS 4206 and NCS 4216 routers.

Interface bandwidth sets and communicates bandwidth value for an interface to higher-level protocols such as OSPFv2 and OSPFv3. Starting with Cisco IOS XE Cupertino Release 17.9.1, when you configure interface bandwidth value for 8-port 10 Gigabit Ethernet Interface module (A900-IMA8Z) and perform triggers such as interface shut or no-shut, IM reload, and Stateful Switchover (SSO), the bandwidth value for the interface is persistently retained. Prior to this release, the bandwidth value would reset to the default value for any trigger.

Configure Bandwidth on Physical Interfaces

To configure bandwidth on the physical interfaces:

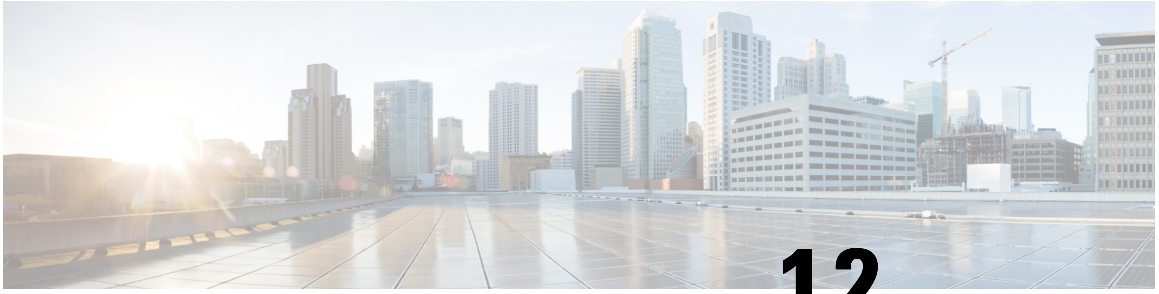
```
!
interface TenGigabitEthernet0/4/6
bandwidth 2000
 ip address 1.1.11.1 255.255.255.224
no shut
!
```

Verify Bandwidth Configuration

Use the **show interface** command to display statistics for the network interfaces.

```
Router#show interface Te0/4/6
TenGigabitEthernet0/4/6 is up, line protocol is up
  Hardware is A900-IMA8Z, address is 00af.1f5a.5ac1 (bia 00af.1f5a.5a94)
  MTU 1500 bytes, BW 2000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

```
Full Duplex, 10000Mbps, link type is auto, media type is 10GBase-SR
output flow-control is unsupported, input flow-control is on
Transport mode LAN
```

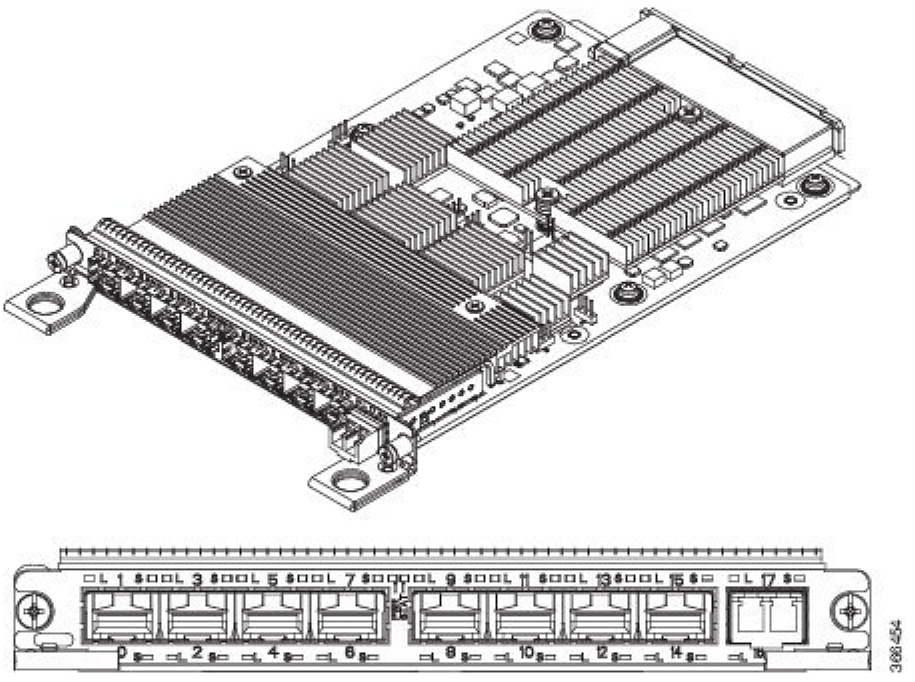


CHAPTER 12

Configuring 8/16-port 1 Gigabit Ethernet (SFP / SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module

The 8/16-port 1 Gigabit Ethernet (SFP / SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module has 8 ports of 1 Gigabit Ethernet and 1 port of 10 Gigabit . The 8/16-port 1 Gigabit Ethernet (SFP / SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module operates on multiple port densities and operating modes. Each physical port can be extended to have 2 ports of 1 Gigabit Ethernet with the use of Compact Small Form-Factor Pluggable (CSFP) module to address high-density port requirements in FTTx deployments.

Figure 4: 8/16-port 1 Gigabit Ethernet (SFP / SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module



Each port on CSFP acts as Transmitter or Receiver and connects to GLC-BX-U SFPs using a single strand fiber. GLC-BX-U SFPs support digital optical monitoring (DOM) functions according to the industry-standard SFF-8472 multisource agreement (MSA). This feature gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

Note CSFP must be connected only to GLC-BX-U.

This interface module has 8 physical ports of 1 Gigabit Ethernet and 1 physical port of 10 Gigabit Ethernet, but with the support of CSFP, it can support a maximum of 18 ports of 1 Gigabit Ethernet. Thus, the interface module offers enhanced bandwidth.

The following table shows the type of SFPs for 1G and 10G Modules.

Table 19: Type of SFPs for 1G and 10G Modules

Module	Optics
1G Module	SFP
	CSFP
10G Module	SFP+
	SFP
	CSFP

Operating Modes

The interface module supports the following two operating modes:

- Full Subscription
- Over Subscription

Note The interface module supports 8 ports of 1 Gigabit Ethernet + 1 port of 10 Gigabit Ethernet mode by default (except the slots 0, 1, 6, and 9 with XFI Pass through mode).

Full Subscription Mode

Full subscription operating mode supports the bandwidth equal to the number of ports configured.

For example, if you configure 8-port 1GE + 1-port 10GE in full subscription operating mode, then the supported bandwidth is 8 Gigabit Ethernet and 10 Gigabit Ethernet.

The supported operating modes of Full Subscription for ASR 903 NCS 4206 Routers are:

- 16-port 1GE + 1-port 10GE
- 8-port 1GE + 1-port 10 GE
- 18-port 1GE

The supported operating modes of Full Subscription for ASR 907 NCS 4216 Routers are:

- 8-port 1GE + 1-port 10GE
- 8-port 1GE + 1-port 1GE
- 8-port 1GE
- 1-port 10GE

Over Subscription Mode

Over Subscription operating mode is applicable to 1 Gigabit Ethernet ports only. 16-port 1GE and 16-port 1GE + 1-port 10GE operating modes support 8 Gigabit Ethernet and 18 Gigabit Ethernet bandwidth, respectively. 18-port 1GE supports 9 Gigabit Ethernet bandwidth. But, if the total bandwidth exceeds the supported bandwidth, it results in low priority traffic drop.

For example, if you configure 16-port 1GE + 1-port 10GE over subscription operating mode, then 8GE bandwidth is suported for 16 ports of 1 Giagabit Ethernet and 10GE bandwidth is supported for 10 Giagabit Ethernet ports.

The following are the supported operating modes of Over Subscription for NCS 4216 Routers:

- 16-port 1GE
- 16-port 1GE + 1-port 10GE
- 18-port 1GE

Note In 18-port 1GE mode, 10 Gigabit Ethernet physical port slot becomes 2 ports of 1 Gigabit Ethernet with insertion of CSFP.

Note By default, the interface module loads in 8-port 1GE + 1-port 10 GE modes (except the slots 0, 1, 6, and 9 with XFI-Pass Through mode. For more information, refer Optics Matrix.

Note Over subscription mode is *not* supported on NCS 4206 Routers.

Traffic is classified as follows:

- High Priorty Traffic — Has high priority queue

  This is classified as follows:

  - DMAC=01-80-C2-xx-xx-xx
  - Etype=0x8100, 9100, 9200, 88A8 Cos values=5, 6, 7
  - Etype=0806 (ARP), 88F7 (PTP)
  - Etype=0x800, TOS 5, 6, 7
  - Etype=0x8847, MPLS EXP 5, 6, 7

- Low Priority Traffic — Traffic that does not satisfy the above conditions has low priority queue

Egress Packet Classifiers

Table 20: Feature History

Feature Name	Release	Description
Oversubscription Support for NCS4200-1T16G-PS	Cisco IOS XE Amsterdam 17.1.1	Egress packet classification is done based on priority-based flow-control (PFC) to ensure that there are no drop in packets.

During oversubscription, the egress direction classifies the packet based on the following:

- The first 8 ports use the priority-based flow-control (PFC) to ensure that there are no drop in packets.
- The remaining ports do strict priority between High Priority and Low Priority counters.

Note The threshold value is 6 by default (packet with CoS/EXP/DSCP value greater than or equal to 6 is classified as High Priority.

SADT Mode

For more information on SADT mode, see IP SLAs Configuration Guide, Cisco IOS XE 17.

Bandwidth Mode

Each interface module subslot can be assigned a bandwidth. You can reserve the slots with specific bandwidth so that the inetrface module that consumes more than the configured bandwidth is not used.

The following table shows the interface module slots for the bandwidth mode.

IM Subslot	Bandwidth Mode	SADT Operating Mode
0	8 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	10 Gbps	XFI-Pass Through Mode
1	8 Gbps	Port Expansion Mode
	10 Gbps	XFI-Pass Through Mode
2	8 Gbps	Port Expansion Mode
	10 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	18 Gbps	Port Expansion Mode
	20 Gbps	XFI-Pass Through Mode
3	Not Available	NA
4	Not Available	NA
5	8 Gbps	Port Expansion Mode
	10 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	18 Gbps	Port Expansion Mode
	20 Gbps	XFI-Pass Through Mode
6	8 Gbps	Port Expansion Mode
	10 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	18 Gbps	Port Expansion Mode

IM Subslot	Bandwidth Mode	SADT Operating Mode
7	80 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	100 Gbps	Port Expansion Mode or XFI-Pass Through Mode
8	80 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	100 Gbps	Port Expansion Mode or XFI-Pass Through Mode
9	8 Gbps	Port Expansion Mode
	10 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	18 Gbps	Port Expansion Mode
10	8 Gbps	Port Expansion Mode
	10 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	18 Gbps	Port Expansion Mode
	20 Gbps	XFI-Pass Through Mode
11	Not Available	NA
12	Not Available	NA
13	8 Gbps	Port Expansion Mode
	10 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	18 Gbps	Port Expansion Mode
	20 Gbps	XFI-Pass Through Mode
14	8 Gbps	Port Expansion Mode
	10 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	18 Gbps	Port Expansion Mode
	20 Gbps	XFI-Pass Through Mode

IM Subslot	Bandwidth Mode	SADT Operating Mode
15	8 Gbps	Port Expansion Mode
	10 Gbps	Port Expansion Mode or XFI-Pass Through Mode
	18 Gbps	Port Expansion Mode
	20 Gbps	XFI-Pass Through Mode

Slot Support on Operating Modes

The following table shows the slots supported on different operating modes on NCS 4216 Routers.

IM Subslot	SADT Operating Mode	IM Operating Modes
0, 1	Port Expansion Mode	Unsupported
	XFI-Pass Through Mode	8-port 1GE + 1-port 1GE
		8-port 1GE
		16-port 1GE Over Subscribed
		18-port 1GE Over Subscribed
2, 5, 10, 13, 14, 15	XFI-Pass Through Mode	8-port 1GE + 1-port 10GE
		16-port 1GE + 1-port 10GE Over Subscribed
	Any	8-port 1GE + 1-port 1GE
		8-port 1GE
		16-port 1GE Over Subscribed
		18-port 1GE Over Subscribed
		1-port 10GE

IM Subslot	SADT Operating Mode	IM Operating Modes
3, 4, 7, 8, 11, 12	Any	8-port 1GE + 1-port 10GE
		8-port 1GE + 1-port 1GE
		8-port 1GE
		1-port 10GE
		16-port 1GE + 1-port 10GE Over Subscribed
		16-port 1GE Over Subscribed
		18-port 1GE Over Subscribed
6, 9	Any	8-port 1GE + 1-port 1GE
		8-port 1GE
		1-port 10GE
		16-port 1GE Over Subscribed
		18-port 1GE Over Subscribed

IOS Port Numbering

The IOS port numbers are different from other typical interface module because of the flexibility of optics choices and operating modes. The IOS port number is even numbered for SFP optics (for example, Gigabit Ethernet 0/x/0) and the additional port on CSFP insertion introduces the odd number (for example, Gigabit Ethernet 0/x/0 and Gigabit Ethernet 0/x/1) as enumerated in the table below.

Table 21: IOS Port Number

1G Face Plate Port	SFP Optics	CSFP Optics
0	Gigabit Ethernet 0/x/0	Gigabit Ethernet 0/x/0 and Gigabit Ethernet 0/x/1
1	Gigabit Ethernet 0/x/2	Gigabit Ethernet 0/x/2 and Gigabit Ethernet 0/x/3
2	Gigabit Ethernet 0/x/4	Gigabit Ethernet 0/x/4 and Gigabit Ethernet 0/x/5
3	Gigabit Ethernet 0/x/6	Gigabit Ethernet 0/x/6 and Gigabit Ethernet 0/x/7
4	Gigabit Ethernet 0/x/8	Gigabit Ethernet 0/x/8 and Gigabit Ethernet 0/x/9

1G Face Plate Port	SFP Optics	CSFP Optics
5	Gigabit Ethernet 0/x/10	Gigabit Ethernet 0/x/10 and Gigabit Ethernet 0/x/11
6	Gigabit Ethernet 0/x/12	Gigabit Ethernet 0/x/12 and Gigabit Ethernet 0/x/13
7	Gigabit Ethernet 0/x/14	Gigabit Ethernet 0/x/14 and Gigabit Ethernet 0/x/15

Similarly, the IOS port number on the 10G module also has an even number and the additional port on CSFP insertion is odd numbered as listed in the table below.

Table 22: IOS Port Number

10G Face Plate Port	SFP+	SFP (1G BW)	CSFP (1G BW)
8	Ten Gigabit Ethernet 0/x/16	Ten Gigabit Ethernet 0/x/16	Ten Gigabit ethernet 0/x/16 and Gigabit Ethernet 0/x/17

Suported Features on the Interface Module

- Supports PTP implementation. PTP is supported on 1G SFP, 10G SFP+, and CSFP ports.
- Supports SyncE.
- Supports both full subscription and over subscription modes.
- Provides multiple combinations of port density in Full subscription and Over Subscription modes.

Benefits

- The interface module has enhanced port density.
- 10 GE port can also operate in 1GE mode.

Restrictions

- In XFI Pass through mode, the interface module goes out of service without any mode configuration on slots 0, 1, 6, and 9. Configure the supported modes on the slots before inserting the interface module.
- This interface module is supported only on Cisco RSP3 module.
- OTN, Wan Phy, and MACsec are *not* supported.
- High Priority Traffic with frame size more than 4500 bytes is *not* supported for oversubscription mode.

- COS, EXP, and DSCP fields in frames with values 5, 6, and 7 respectively, are considered as High Priority Traffic for Oversubscription mode than other control packets.
- 1 G Module ports must have symmetric configuration on both local and peer ends for the ports to come up on the router. For example, if autonegotiation is configured on the local end, it must be configured on the peer end.
- You must wait for 240 seconds between two successive mode changes.

Configuring Interface Module

To configure interface module:

```
enable
hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface GigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
configure terminal
platform hw-module configuration
hw-module 0/4  NCS4200-1T16G-PS mode mode
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface GigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
```

Example: Configuring Full Subscription Modes

The following are the examples to configure different modes of full subscription.

8-port 1GE + 1-port 10GE Full Subscription Mode Configuration:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 8x1G+1x10G-FS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

8-port 1GE + 1-port 1GE Full Subscription Mode Configuration:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 8x1G+1x1G-FS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
```

8-port 1GE Full Subscription Mode Configuration:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 8x1G-FS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

1-port 10GE Full Subscription Mode Configuration:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
```

```
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 1x10G-FS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

Example: Configuring Over Subscription Modes

The following are the examples to configure different modes of over subscription.

16-port 1GE + 1-port 10GE Over Subscription Mode Configuration:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 16x1G+1x10G-OS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
```

```
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

18-port 1GE Over Subscription Mode Configuration:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 18x1G-OS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

16-port 1GE Over Subscription Mode Configuration:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)#platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 16x1G-OS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

Example: Configuring Egress Classification

Note PFC (priority-based flow-control) and egress classification are enabled by default.

The following configuration shows how to modify an egress classification:

```
int gi 0/15/8
flowcontrol egress classify all threshold 7

flowcontrol egress classify ?
            all   classify based on L2-CoS, MPLS-EXP and L3-DSCP
            l2    classify based on L2-CoS
            l3    classify based on L3-DSCP precedence bits
            mpls  classify based on MPLS-EXP

qos-overhead-accounting enable gigabitEthernet 0/15/1
qos-overhead-accounting positive 4
```

Verifying PFC

Use the show platform hardware pp active bshell command to verify the PFC (priority-based flow-control).

```
show platform hardware pp active bshell "show counters full"
T_127.xl7                     :         1,410,242,436             +2,365
903/sTPOK.xl7                 :         1,410,242,436             +2,365
903/sTPKT.xl7                 :         1,410,242,436             +2,365
903/sTUCA.xl7                 :         1,410,242,436             +2,365
903/sTBYT.xl7                 :        95,896,485,648           +160,820
61,375/sR_64.xe134            :               390,320               +786
299/sRPKT.xe134               :               916,242               +786
299/sRXCF.xe134               :               390,320               +786
299/sRXPP.xe134               :               390,320               +786
299/sRPFC_0.xe134             :               362,115               +786
299/sRPFC_1.xe134             :               362,925               +786
299/sRPFC_2.xe134             :               361,555               +786
299/sRPFC_3.xe134             :               362,454               +786
299/sRPFC_4.xe134             :               363,298               +786
299/sRPFC_5.xe134             :               361,532               +786
299/sRPFC_6.xe134             :               362,606               +786
299/sRPFC_7.xe134             :               362,034               +786
299/sRBYT.xe134               :           100,972,834            +50,304
```

Verifying Configuration

Use the **show platform hw-configuration** command to verify the operating modes configured on the interface module.

```
Router#show platform hw-configuration
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State Op Mode
BW
------ ------------------- ------------------- ------------------ -------- ------------
------------        --
 0/0   -                   -                   Empty              N/A      -

 0/1   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G-OS
 0/2   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       18x1G-OS

 0/3   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G

 0/4   -                   -                   Empty              N/A      -

 0/5   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       18x1G-OS

 0/6   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G-OS

 0/7   -                   -                   Empty              N/A      -

 0/8   -                   -                   Empty              N/A      -

 0/9   -                   -                   Empty              N/A      -

 0/10  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS

 0/11  -                   -                   Empty              N/A      -

 0/12  -                   -                   Empty              N/A      -

 0/13  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS

 0/14  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS

 0/15  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS
```

```
Router#show platform hw-configuration
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State Op Mode
BW
------ ------------------- ------------------- ------------------ -------- ------------
--
 0/0   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/1   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/2   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/3   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G

 0/4   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/5   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/6   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/7   -                   NCS4200-1H-PK       IS-NR              IS       -

 0/8   -                   NCS4200-1H-PK       IS-NR              IS       -

 0/9   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/10  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/11  -                   -                   Empty              N/A      -

 0/12  -                   -                   Empty              N/A      -

 0/13  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/14  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS
 0/15  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS
```

Verifying High Priority and Low Priority Counters Configuration

Use **show platform software agent iomd** [*IM module*] **fpga dump** [*port number*] to display the packets of High Priority and Low Priority traffice queue in Over Subscription mode.

```
#show platform software agent iomd 0/8 fpga dump 4
OS LP Drop Q Pkt Cnt :0x0
OS HP Drop Q Pkt Cnt :0x0
OS LP Q Pkt Cnt :0x22906bd0
OS HP Q Pkt Cnt :0x55fdd731
```

Use **show platform software agent iomd** [*IM module*] **fpga clear** [*port number*] to clear High Priority and Low Priority counters in Over Subscription mode.

```
#show platform software agent iomd 0/8 fpga clear 4
OS LP Drop Q Pkt Cnt :0x0
OS HP Drop Q Pkt Cnt :0x0
OS LP Q Pkt Cnt :0x0
OS HP Q Pkt Cnt :0x0
```

Configuring Bandwidth Mode

To configure bandwidth mode:

```
enable
configure terminal
platform hw-module configuration
bandwidth 0/0 8-gbps
end
```

Verifying Bandwidth Mode Configuration

Use `show platform hw-configuration` command to verify bandwidth mode configuration.

```
#show platform hw-configuration
Slot   Cfg IM Type          Actual IM Type       Op State           Ad State Op Mode      BW

------ ------------------- ------------------- ------------------ -------- ------------ --
 0/0   -                    -                    Empty              N/A      -
 0/1   A900-IMA8CS1Z-M      A900-IMA8CS1Z-M      IS-NR              IS       16x1G-OS
 0/2   A900-IMA8CS1Z-M      A900-IMA8CS1Z-M      IS-NR              IS       18x1G-OS
 0/3   A900-IMA8CS1Z-M      A900-IMA8CS1Z-M      IS-NR              IS       16x1G+1x10G
 0/4   -                    -                    Empty              N/A      -
 0/5   A900-IMA8CS1Z-M      A900-IMA8CS1Z-M      IS-NR              IS       18x1G-OS
20-gbps
 0/6   A900-IMA8CS1Z-M      A900-IMA8CS1Z-M      IS-NR              IS       16x1G-OS
 0/7   -                    -                    Empty              N/A      -
 0/8   -                    -                    Empty              N/A      -
 0/9   -                    -                    Empty              N/A      -
 0/10  A900-IMA8CS1Z-M      A900-IMA8CS1Z-M      IS-NR              IS       16x1G+1x10G-OS
 0/11  -                    -                    Empty              N/A      -
 0/12  -                    -                    Empty              N/A      -
 0/13  A900-IMA8CS1Z-M      A900-IMA8CS1Z-M      IS-NR              IS       16x1G+1x10G-OS
 0/14  A900-IMA8CS1Z-M      A900-IMA8CS1Z-M      IS-NR              IS       16x1G+1x10G-OS
 0/15  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS
#

#show platform hw-configuration
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State Op Mode
BW
------ ------------------- ------------------- ------------------ -------- ------------
--
 0/0   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS
10-gbps
 0/1   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/2   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G

 0/3   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G

 0/4   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/5   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/6   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/7   -                   NCS4200-1H-PK       IS-NR              IS       -

 0/8   -                   NCS4200-1H-PK       IS-NR              IS       -

 0/9   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/10  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/11  -                   -                   Empty              N/A      -

 0/12  -                   -                   Empty              N/A      -

 0/13  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/14  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/15  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS
```

Interface Module Rules

NCS 4206 Routers or Cisco RSP3C-400-S Rules for NCS4200-1T16G-PS

Slot Number	Supported IM Operating Modes	Restrictions
0	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16 x 1GigE (CSFP) + 1 x 10GigE (SFP+) Fully subscribed • 18-port 1GE Fully subscribed	The IM cannot be in slot 0 if IMA1C is in slot 4. If the IM is in slot 0, then it does not allow 100G IM to be inserted in slots 4 and 5.

Slot Number	Supported IM Operating Modes	Restrictions
1	Not Supported	—
2	Not Supported	—
3	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1 x 10GE (SFP+) Fully subscribed • 18-port 1GE Fully subscribed	—
4	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Fully subscribed • 18-port 1GE Fully subscribed	—
5	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Fully subscribed • 18-port 1GE Fully subscribed	—

NCS 4216 ASR 907 Routers or Cisco RSP3C (Port Expansion Mode) Rules for A900-IMA8CS1Z NCS4200-1T16G-PS

Note

- If IMA8S, IMA8T, IMA8S1Z, and IMA8T1Z are in any slot, SADT cannot be configured.
- If the IMA8CS1Z interface module is not present in a slot, mode update through hw sub-slot mode is not allowed. The existing mode configuration applies to the interface module that is reinserted, and you can subsequently update the mode.

Slot Number	Supported IM Operating Modes	Restrictions
0	Not supported	—

Slot Number	Supported IM Operating Modes	Restrictions
1	Not supported	—
2	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10GE Fully subscribed	For Slot 2 in 8-port 1GE Fully Subscribed or 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode, IMA8Z or IMA2F cannot be in slot 4.
3	All modes are supported	If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15.
4	All modes are supported	If IMA8Z or IMA2F is present in slot 4, the IM cannot be used in slots 2, 6, 10 and 14.
5	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10G Fully subscribed	If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15.
6	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10G Fully subscribed	If IMA8Z or IMA2F is present in slot 4, the IM cannot be used in slots 2, 6, 10 and 14.
7	All modes are supported	—
8	All modes are supported	—

Slot Number	Supported IM Operating Modes	Restrictions
9	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10G Fully subscribed	If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15.
10	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10G Fully subscribed	If IMA8Z or IMA2F is present in slot 4, the IM cannot be used in slots 2, 6, 10 and 14.
11	All modes are supported	If the IM is in slot 11, IMA8S, IMA8T, IMA8S1Z, and IMA8T1Z cannot be used in slots 1, 5, 9, 13 and 15.
12	All modes are supported	If the IM is in slot 12, IMA8S, IMA8T, IMA8S1Z, and IMA8T1Z cannot be used in slots 0, 2, 6, 10 and 14.
13	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10G Fully subscribed	If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15.

Slot Number	Supported IM Operating Modes	Restrictions
14	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10G Fully subscribed	If IMA8Z or IMA2F is present in slot 4, the IM cannot be used in slots 2, 6, 10 and 14.
15	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10G Fully subscribed	If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15.

NCS 4216 ASR 907 Routers or Cisco RSP3C (XFI-Pass Through Mode) for A900-IMA8CS1Z NCS4200-1T16G-PS

Note IMA8S, IMA8T, IMA8S1Z, and IMA8T1Z cannot be used in any slot.

Slot Number	Supported IM Operating Modes	Restrictions
0	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed	• If the IM is in slot 0 in 8-port 1GE Fully subscribed mode or in 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, the IM in Slot 12 can only be in 8-port 1GE (SFP) Fully subscribed mode or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, 1-port 10GE Fully subscribed mode. • If Slot 0 is in 8-port 1G Fully subscribed mode or 16-port/18-port 1GE, or 16-port/18-port 1G Over subscribed or 1-port 10G Fully subscribed mode or 8-port 1G + 1-port 1G Fully subscribed mode. • If Slot 0 is in 8-port 1G Fully subscribed mode or 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, then IMA8Z or IMA2F cannot be in slot 12. • IF IMA8CS1Z-M is in slot 0, then NCS4200 1T8S-10CS (10G_CEM) in slot 12 is not supported. • IF IMA8CS1Z-M is in slot 0 then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported.
1	• 8-port 1GE (SFP) Fully subscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed	• If Slot 1 is in 8-port 1G Fully subscribed or 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, the IMA8Z or IMA2F or IMA2Z cannot be in slot 11. • If the IM is in slot 1, then NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported. • If the IM is in slot 1, then NCS4200-1T8S-10CS (5G_CEM) in slot 11 is supported.

Slot Number	Supported IM Operating Modes	Restrictions
2	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed • 16-port/18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10G Fully subscribed • 8-port 1GE Fully subscribed	• If Slot 2 is in 8-port 1G + 1-port 10G Fully subscribed mode, or 16-port 1G + 1-port 10G Over subscribed mode, then no IM can be present in slot 12. • If Slot 2 is in 8-port 1G + 1-port 10G Fully subscribed mode, or 16-port 1G + 1-port 10G Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 4. • If the IM in slot 2, then NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported. • If the IM is in slot 2, then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is not supported. • If the IM is in slot 2 then NCS4200-48T1E1-CE in slot 12 is not supported. • If the IM is in slot 2 then NCS4200-48T3E3-CE in slot 12 is not supported.
3	All modes are supported.	• If IMA8Z or IMA2F is in slot 3, then the IM is not supported on slots 5, 9, 13, and 15. • If Slot 3 has IMA8Z or IMA2F, then no IM can be present in slots 5, 9, 13, and 15.
4	All modes are supported.	• If IMA8Z or IMA2F is in slot 4, then the IM is not supported in slots 2, 6, 10, and 14. • If Slot 4 has IMA8Z or IMA2F, then no IM can be present in slots 2, 6, 10, and 14.
5	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Over subscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10GE Fully subscribed • 8-port 1GE Fully subscribed	• If the IM is in slot 5 in 8-port 1GE + 1-port 10GE Fully subscribed mode or in 16-port 1GE + 1-port 10GE Oversubscribed mode, the the IM in slot 11 can only be in 8-port 1GE Fully subscribed mode or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, or 1-port 10 GE Fully subscribed mode. • If Slot 5 is in 8-port 1G + 1-port 10G Fully subscribed, or 16-port 1G + 1-port 10G Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 3. • If the IM is in slot 5, then NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported. • If the IM is in slot 5, then NCS4200-1T8S-10CS (5G_CEM) in slot 11 is supported.

Slot Number	Supported IM Operating Modes	Restrictions
6	• 8-port 1GE (SFP) Fully subscribed mode • 16-port 1GE (CSFP) Oversubscribed • 18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10 GE Fully subscribed	• If Slot 6 is in 8-port 1GE fully subscribed, or 16-port 1GE Over subscribed, or 18-port 1GE Over subscribed or 8-port 1GE + 1-port 1GE fully subscribed or 1-port 10GE Fully subscribed mode, then IMA8Z or IMA2F cannot be in slot 4.
7	All modes are supported	—
8	All modes are supported	—
9	• 8-port 1GE (SFP) Fully subscribed • 16-port/18-port 1GE (CSFP) Oversubscribed • 16-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10 GE Fully subscribed	If Slot 9 is in 8-port 1GE fully subscribed, or 16-port 1GE Over subscribed mode, or 18-port 1GE Over subscribed mode or 8-port 1GE + 1-port 1GE fully subscribed or 1-port 10GE Fully subscribed mode, then IMA8Z or IMA2F cannot be in slot 3.
10	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed • 16-port/18-port 1GE (CSFP) Oversubscribed • 8-port 1GE+1-port 1GE Fully subscribed • 1-port 10 GE Fully subscribed • 8-port 1G Fully subscribed	• If Slot 10 and 14 are in 8-port 1GE + 1-port 10GE Fully subscribed, or 16-port 1GE + 1-port 10GE Over subscribed mode, then IMA8Z IMA2F cannot be in Slot 4. • If IM is in slot 10 then NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported. • If IM is in slot 10, then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported.

Slot Number	Supported IM Operating Modes	Restrictions
11	All modes are supported	

Slot Number	Supported IM Operating Modes	Restrictions
		• IM can be in slot 11, only in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, or 1-port 10 GE Fully subscribed mode if IPSEC is used (FLSASR907-IPSEC). • If the IM is slot 11, and in 8-port 1GE + 1 x 10GigE Fully subscribed mode, or in 16-port 1GE + 1-port 10GE Oversubscribed mode, then the IM in Slots 5 and 15 can only be in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE +1-port 1GE Fully subscribed or 1-port 10GE Fully subscribed mode. • If the IM is in slot 11, and in 8-port 1GE Fully subscribed mode, or in 16-port 1GE Oversubscribed mode, or in 18-port 1GE Oversubscribed mode or in 8-port 1GE + 1-port 1GE Fully subscribed or 1-port 10GE Fully subscribed, then the IM in Slot 15 can only be in 8-port 1GE (SFP) Fully subscribed mode, OR in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 1-port 10GE Fully subscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode. • IF IMA2Z is in slot 11, then the IM is in slot 15 only in 8-port 1GE (SFP) Fully subscribed mode, OR in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode, and no IM can be present in slot 1. • If IMA8Z or IMA2Fis in slot 11, then the IM is in slots 5, 13 and 15 in 8-port 1GE Fully Subscribed, or in 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode, and no IM can be present in slot 1. • If NCS4200-1T8S-10CS (10G_CEM) is in slot 11, then the IM in slots 5, 13 and 15 are in only 8-port 1GE Fully Subscribed, or in 16/18-port 1GE Oversubscribed mode, and the IM in slot 1 not supported. • If NCS4200-1T8S-10CS (5G_CEM) is in slot 11, then the IM in slot 15 is in only 8-port 1GE Fully Subscribed, OR in 16/18-port 1GE Oversubscribed mode. • If NCS4200-48T1E1-CE is in slot 11, then the IM is in slot 15 is in only 8-port 1GE Fully Subscribed, or

Slot Number	Supported IM Operating Modes	Restrictions
		in 16/18-port 1GE Oversubscribed mode. • If NCS4200-48T3E3-CE is in slot 11, then the IM is in slot 15 is in only 8-port 1GE Fully Subscribed, or in 16-port/18-port 1GE Oversubscribed mode.

Slot Number	Supported IM Operating Modes	Restrictions
12	All modes are supported	

Slot Number	Supported IM Operating Modes	Restrictions
		• If the IM is in slot 12, and in 8-port 1GE + 1-port 10GE Fully subscribed mode, or in 16-port 1GE + 1-port 10GE Oversubscribed mode, then no IM can be present in Slot 0, and the IM in Slot 2 can only be in 8-port 1GE (SFP) Fully subscribed mode, OR in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode. • If the IM is in slot 12 and in 8-port 1GE Fully subscribed mode or in 16-port 1GE Oversubscribed mode, or in 18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode, then the IM in Slot 2 can only be in 8-port 1GE (SFP) Fully subscribed mode, OR in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode. • IF IMA2Z is in slot 12, then the IM is in slots 2 and 10 in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode. • If Slot 12 has IMA2Z, then slots 2 and 10 in 8-port 1GE Fully subscribed mode, or 16-port/18-port 1GE Over subscribed mode or 1-port 10GE Fully subscribed mode or 8-port 1G + 1-port 1GE Fully subscribed mode. • If IMA8Z OR IMA2F is in slot 12, then the IM in slots 2, 10 and 14 in 8-port 1GE Fully Subscribed, or in 16-port/18-port 1GE Oversubscribed mode and 1-port 10GE Fully subscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, and no IM can be present from Slot 1 to Slot 0. • If NCS4200-1T8S-10CS (10G_CEM) is in slot 12, then the IM in slots 2, 10 and 14 are in only 8-port 1GE Fully Subscribed, OR in 16-port/18-port 1GE Oversubscribed mode, and the IM in slot 0 not supported. • If NCS4200-1T8S-10CS (5G_CEM) is in slot 12, then the IM in slot 2 is in only 8-port 1GE Fully Subscribed, OR in 16-port/18-port 1GE Oversubscribed mode. • If NCS4200-48T1E1-CE is in slot 12, then the IM in slot 2 is in only 8-port 1GE Fully Subscribed, OR in 16-port/18-port 1GE Oversubscribed mode.

Slot Number	Supported IM Operating Modes	Restrictions
		• If NCS4200-48T3E3-CE is in slot 12, then the IM in slot 2 is in only 8-port 1GE Fully Subscribed, or in 16-port/18-port 1GE Oversubscribed mode.
13	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed • 16-port/18-port 1GE (CSFP Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10 GE Fully subscribed • 8-port 1G Fully subscribed	• If IPSEC is used (FLSASR907-IPSEC) then the IM can be in slot 13, only in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode. NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported; but NCS4200-1T8S-10CS (5G_CEM) in slot 11 is supported. • If the IM in slot 13 is configured in 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed mode, or in 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed mode, or Fully Subscribed mode, then IPSEC cannot be configured. If Slot 13 is in 8-port 1GE + 1-port 10GE Fully subscribed mode, or 16-port 1GE + 1-port 10GE Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 3. • If the IM is in slot 13, then NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported. • If the IM is in slot 13, then NCS4200-1T8S-10CS (5G_CEM) in slot 11 is supported.
14	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed • 16-port/18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10 GE Fully subscribed • 8-port 1GE Fully subscribed	• IF 10G Y.1564/SADT is used, then the IM can be in slot 14 only in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode, or 8-port 1GE + 1-port 1GE Fully subscribed mode, or 1-port 10GE Fully subscribed mode. NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported, but NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported. • If Slot 14 is in 8-port 1GE + 1-port 10GE Fully subscribed mode or 16-port 1GE + 1-port 10GE Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 4. • If the IM is in slot 14, then NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported. • If the IM is in slot 14, then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported.

Slot Number	Supported IM Operating Modes	Restrictions
15	• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed • 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed • 16-port/18-port 1GE (CSFP) Oversubscribed • 8-port 1GE + 1-port 1GE Fully subscribed • 1-port 10 GE Fully subscribed • 8-port 1GE Fully subscribed	• IF IMA8CS1Z-M is in slot 15 in 8-port 1GE + 1-port 10GE Fully subscribed mode, or in 16-port 1GE + 1-port 10GE Oversubscribed mode, then the IM cannot be present in slot 11. • If Slot 15 is in 8-port 1GE + 1-port 10GE Fully subscribed mode, or 16-port 1GE + 1-port 10GE Over subscribed mode, then no IM is supported on slot 11. • If Slot 15 is in 8-port 1GE + 1-port 10GE Fully subscribed, Or 16-port 1GE + 1-port 10GE Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 3. • If the IM is in slot 15, then NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported. • If the IM is in slot 15, then NCS4200-1T8S-10CS (5G_CEM) in slot 11 is not supported. • If the IM is in slot 15, then NCS4200-48T1E1-CE in slot 11 is not supported. • If the IM is in slot 15, then NCS4200-48T3E3-CE in slot 11 is not supported.

8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module Support in Slots 1 and 2 for NCS 4206 Router

Table 23: Feature History

Feature Name	Release Information	Feature Description
8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module Support in Slots 1 and 2	Cisco IOS XE Cupertino 17.7.1	This feature introduces the support of the 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) interface module on slots 1 and 2 and thus enables the port expansion in XFI pass through mode.

Prior to Cisco IOS XE Cupertino 17.7.1 release, the 8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) interface module was only supported on slots 0, 3, 4, and 5.

Starting with Cisco IOS XE Cupertino 17.7.1 release, the interface module is additionally supported on slots 1 and 2. This support enables port expansion and thus you can now use 16X1G and 18X1G ports.

Note This feature is *only* supported on NCS 4206 routers.

Operating Modes

The following table lists the interface module operating modes for NCS 4206 router.

Table 24: Operating Modes

Per Slot Supported Operating Modes	
Interface Module Subslots	**Interface Module Operating Modes**
0, 1, 2, 3, 4, and 5	16X1G+1X10G Fully Subscribed
	8X1G+1X10G
	18X1G Fully Subscribed

Restrictions

- This feature is only supported in XFI pass through mode.
- In port expansion mode, the interface module goes out of service on slots 1 and 2.

Configure XFI Pass Through Mode

To configure XFI pass through mode and bring up the interface module in slots 1 and 2:

```
Router(config)# license feature service-offload enable
Please write the configuration and issue reload for effecting the configuration
Router(config)# license feature service-offload bandwidth 10gbps npu-0
Router(config)#end
```

Verification of XFI Pass Through Mode Configuration

Use the **show platform** command to verify the XFI pass through mode configuration for slots 1 and 2:

```
Router#show platform
Chassis type: NCS4206-SA

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      NCS4200-1T16G-PS    ok                    00:02:01
 0/1      NCS4200-1T16G-PS    ok                    00:02:01
 0/2      NCS4200-1T16G-PS    ok                    00:02:01
 0/3      NCS4200-8T-PS       ok                    00:02:01
 0/5      NCS4200-1H-PK       ok                    00:02:01
R0        NCS420X-RSP         ok, active            00:10:10
```

```
R1        NCS420X-RSP         init, standby        00:10:10
F0                            ok, active           00:10:10
F1                            init, standby        00:10:10
P0        A900-PWR550-A       ok                   00:06:26
P1        A900-PWR550-A       ok                   00:06:22
P2        A903-FAN-E          ok                   00:06:35

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        19052734            15.6(49r)S
R1        19052734            15.6(49r)S
F0        19052734            15.6(49r)S
F1        19052734            15.6(49r)S
```

Associated Commands

The following table shows the Associated Commands for interface module configuration:

Commands	Links
show platform software agent iomd [*im module*] **dump fpga** [*port number*]	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s5.html#wp6318513600
show platform software agent iomd [*im module*] **clear fpga** [*port number*]	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s5.html#wp6318513600

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Compact-SFP	Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet

Standards and RFCs

Standard/RFC	Title
—	*There are no standards and RFCs for this feature.*

MIBs

MIB	MIBs Link
—	*There are no MIBs for this feature.* http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

CHAPTER 13

Using Zero Touch Provisioning

The router provides you the option of having the router auto configure. Field technicians need only mount the router, connect to the power and attach cables in easily-accessible ports, and initiate zero touch provisioning. This feature helps operators to reduce total cost of ownership (TCO) by simplifying the network deployment.

Note ZTP is supported only on the RSP3 module on the NCS 4206-16 Series routers.

ZTP is supported on the NCS 4201-4202 routers.

Note Routers running ZTP must be able to connect to a DHCP server and a TFTP server, download the configuration template, and begin operation.

Note ZTP must be initiated only from the R0 that has the active RSP module in a dual RSP scenario.

Prerequisites for Using ZTP

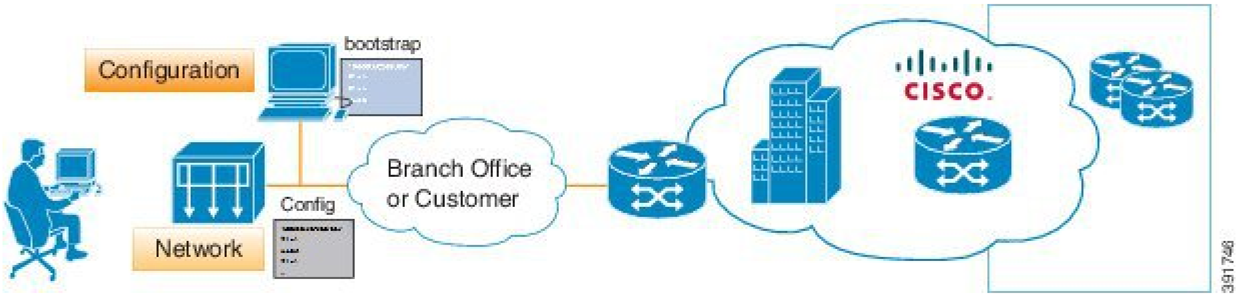
- The connection between the DHCP server or relay and TFTP server and router must be established.
- The TFTP server must have the required network configuration file stored and should be accessible to the router.

Restrictions for Using ZTP

- ZTP is not supported on the LAN Management port—Gig0 on the router. ZTP is supported only on the Ethernet interfaces such as 1—Gige, 10—Gige ports, and so on.
- ZTP is also not initialized when the router is already reloading or if the router is in ROMMON prompt.
- After the ZTP process completes, you must save the configs using write memory and then reload the router.
- ZTP is not initialized if bootflash has files named as 'router-confg'.
- Disabling gratuitous ARP is not supported.

Information About Using ZTP

Figure 5: Sample ZTP Topology



ZTP is triggered under any of the following conditions:

- A router without a start up configuration is powered on
- The **write erase** and **reload** commands are executed
- The **test platform hardware pp active ztp init** command is executed

The router does *not* have a ZTP or Reset button.

```
Router# write erase
System configuration has been modified. Save? [yes/no]: no
Router# reload
```

Note If you type **yes** at the prompt, the system configuration is saved in the nvRAM and the ZTP process terminates.

After the ZTP process initializes, the following sequence is initiated:

1. The router waits for any of the following packet types through data ports to detect the management VLAN:
    - Broadcast (Gratuitous ARP)
    - ISIS hello packets

- OSPF hello packets
- IPv6 router advertisement packets
- VRRP

Note The operations center can initiate any of the above packets over the network to establish a connection to the DHCP server.

2. When the first packet on any VLAN is detected, the router initiates a DHCP session to a DHCP server over that VLAN.
3. After a DHCP session is established, the router uses the DHCP option 150 and initiates to download a configuration file from the TFTP server. The configuration file in the TFTP server should have anyone of the following naming format:
   a. PID-*chassis-mac-address*

      The PID specifies NCS and *chassis-mac-address* specifies the unique chassis MAC address printed on the chassis. For example, if the chassis mac-address is 00-01-02-03-04-06, then the config file would be NCS-00-01-02-03-04-05.

   b. network-confg
   c. router-confg
   d. ciscortr.cfg
   e. cisconet.cfg

When the ZTP process initiates, the router creates an Ethernet flow point (EFP) and associates a bridge domain interface (BDI) on the detected management VLAN.

The router creates the following configuration to establish a connection with the DHCP server and the TFTP server. The BDI created for this purpose has description **ZTP_BDI** configured under the BDI interface.

Note Once the configuration file is downloaded successfully, you must save the configuration file (write memory) and reload the router.

Caution You may choose to remove the **ZTP_BDI** configuration before reloading the router.

Example ZTP Configuration

Let us assume that GigabitEthernet0/0/1 is connected to the DHCP server and is used to connect to the TFTP server. VLAN ID 1000 is used as the management VLAN.

```
Router# show running-config int gi0/0/1
```

```
Building configuration...
Current configuration : 216 bytes
!
interface GigabitEthernet0/0/1
 no ip address
 media-type auto-select
 no negotiation auto
 service instance 12 ethernet
  encapsulation dot1q 1000
  rewrite ingress tag pop 1 symmetric
  bridge-domain 12
 !
end
!
interface BDI12
description ZTP_BDI
 ip address dhcp
end
```

Downloading the Initial Configuration

After the VLAN discovery process is complete, the configuration download process begins. The following sequence of events is initiated.

1. The router sends DHCP discover requests on each Ethernet interface. The serial number of the router is used as a client identifier.
2. The DHCP server allocates and sends an IP address, TFTP address (if configured with option 150) and default router address to the router.
3. If the TFTP option (150) is present, the router requests a bootstrap configuration that can be stored in any of the following files: , network-confg, router-confg, ciscortr.cfg, or cisconet.cfg.

Note Ensure to use hyphenated hexadecimal notation of MAC address (DOM-78-72-5D-00-A5-80) to name the files.

Note A router running ZTP downloads the configuration from DHCP server. Sometimes, the ZTP DHCP config may already exist as part of network config file. We recommend that you remove the ZTP configuration in the network-confg download file to avoid the router moving into a hung state.

```
ip dhcp pool <pool-number>
network <ip-address> <wildcard-mask>
option 150 ip <ip-address>
 default-router <router-address>
 dns-server <dns-server-address>
```

Effective Cisco IOS XE Amsterdam 17.3.2a, the router tries to learn the reachability to multiple DHCP servers during ZTP. Hence multiple DHCP discovery messages are sent out during this phase. The router goes through all the DHCP offer messages received and selects an appropriate DHCP server based on the priority decided based on below rules:

1. The DHCP server reachable via untagged interface have higher priority than the one via tagged. In case of tagged, the one reachable via an interface learned using VRRP packets has higher priority.
2. If multiple DHCP servers are reachable via similar interfaces mentioned in previous rule, the one reachable via higher physical port number has higher priority.

DHCP Server

The following is a sample configuration to set up a Cisco router as a DHCP server:

```
ip dhcp excluded-address 30.30.1.6
ip dhcp excluded-address 30.30.1.20 30.30.1.255
!
ip dhcp pool mwrdhcp
network 30.30.1.0 255.255.255.0
option 150 ip 30.30.1.6
default-router 30.30.1.6
```

This configuration creates a DHCP pool of 30.30.1.*x* addresses with 30.30.1.0 as the subnet start. The IP address of the DHCP server is 30.30.1.6. Option 150 specifies the TFTP server address. In this case, the DHCP and TFTP server are the same.

The DHCP pool can allocate from 30.30.1.1 to 30.30.1.19 with the exception of 30.30.1.6, which is the DHCP server itself.

TFTP Server

The TFTP server stores the bootstrap configuration file.

The following is a sample configuration (network– confg file):

```
hostname test-router
!
{ncs router-specifc configuration content}
!
end
```

ZTP LED Behavior

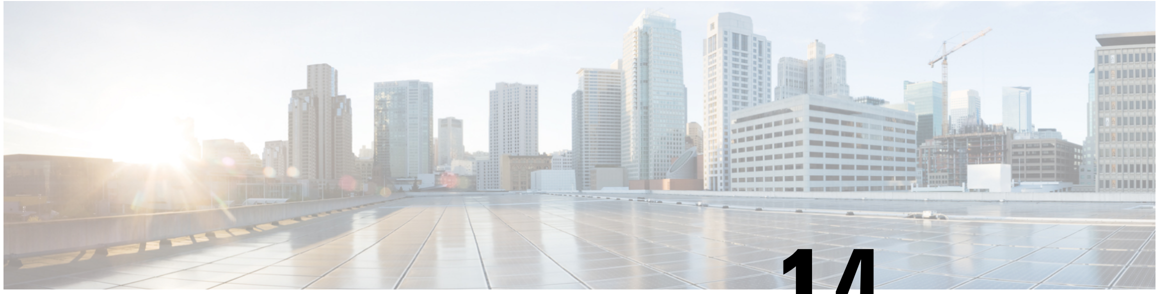
Process	PWR LED	STAT LED
Press ZTP button	Green	Blinking Amber
Loading image	Blinking Green/Red	OFF
Image loaded	Green	Green
ZTP process running	Green	Blinking Amber
ZTP process success and config-file download completes	Green	Green

Process	PWR LED	STAT LED
ZTP process failure or terminated	Green	Red

Verifying the ZTP Configuration

To verify if the ZTP configuration is successful, use the following command:

- **show running-config**



CHAPTER 14

Configuring the SDM Template

This section details the approximate number of resources supported in each templates for a router running the license.

Prerequisites for the SDM Template

Before using an SDM template, you must set the license boot level.

For IPv6 QoS template, the license to use should be *metroipaccess*. You can view the license level using the **show version | in License Level** command

Note If you use *advancedmetroipaccess*, then your options may vary.

Restrictions for the SDM Template

- When using the templates SR 5 label push and SR PFP together, do not use the BDI_MTU template. If the BDI_MTU template is used, then the router may crash continuously, this is applicable from release Cisco IOS XE Amsterdam 17.1.1 to Cisco IOS XE Cupertino 17.9.1. From release Cisco IOS XE Dublin 17.10.1 onwards, during such situation, the router automatically reverts the BDI_MTU template change and performs an additional reboot.
- If you do not enable the EFP feature template, then there is no traffic flow between EFP and VFI (when EFP is with Split Horizon group and VFI is default). But when you enable the EFP feature template, then there is traffic flow between EFP and VFI because of design limitations.
- You cannot edit individual values in a template category as all templates are predefined.

- You cannot use a new SDM template without reloading the router.
- SDM templates are supported only by the Metro Aggregation Services license. Use the help option of the **sdm prefer** command to display the supported SDM templates.
- A mismatch in an SDM template between an active RSP and standby RSP results in a reload of the standby RSP. During reload, SDM template of the standby RSP synchronizes with the SDM template of the active RSP.
- To revert to the current SDM template after using the **sdm prefer** command (which initiates reload of a new SDM template), you must wait for the reload to complete.
- Using the **configure replace** command which results in changes in the current SDM template is not supported.
- The supported group numbers are for scaling in uni-dimension. When scaling in multidimension, the numbers can vary as certain features may share resources.
- When scaling, features using Multiprotocol Label Switching (MPLS) are limited by the number of MPLS labels.
- Internal TCAM usage that is reserved for IPv6 is 133-135 entries. TCAM space that is allotted for SDM template is 135 entries on the router.
- EAID Exhaust occurs when two paths are MPLS and two are IP. It does not occur if all the four paths are IP.
- The following restrictions apply to the maximum IPv6 QoS ACL SDM template:
    - The number of QoS ACL class maps and policy maps that are supported depends on the maximum TCAM entries available.
    - The software solution with expansion is applicable only for maximum QoS SDM template and more than eight Layer 4-port matches are supported for the maximum QoS SDM template. For other templates, due to hardware restriction, a maximum of eight Layer 4-port operators is supported per interface.
    - Ethernet CFM, Ethernet OAM, and Y.1731 protocols are not supported. Features dependent on these protocols are impacted.
    - Layer 2 monitoring features are not supported.
    - The S-TAG based fields are not supported for classification, if IPv6 address match exists in the policy-map.
    - Only eight Layer 4 operations are supported in templates other than maximum IPv6 QoS ACL template.

Note

Release	Time	Activity
16.6.1	49-50 mins	Reload to SSO bulk Sync state
16.7.1	50 mins	Reload to SSO bulk Sync state
16.8.1	-	-
16.9.1	75 mins	Reload to SSO bulk Sync state

Information About the SDM Template

The SDM templates are used to optimize system resources in the router to support specific features, depending on how the router is used in the network. The SDM templates allocate Ternary Content Addressable Memory (TCAM) resources to support different features. You can select the default template to balance system resources or select specific templates to support the required features.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP3.

Table 25: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP3)

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
MAC table	200K	200K	200K
IPv4/VPNv4 Routes	Without MPLS 32k urpf ipv4 routes + 160k ipv4 routes With MPLS 32k urpf ipv4 routes + 160k (ipv4 routes + mpls labels) MPLS Labels = 32000	Without MPLS 192k ipv4 routes With MPLS 192k (ipv4 routes + mpls labels) MPLS Labels = 32000	Without MPLS 76k ipv4 routes With MPLS 76k (ipv4 routes + mpls labels) MPLS Labels = 32000
IPv6/VPNv6 Routes	8192	8192	36864
uRPF IPv4 routes	32768	32768	32768
IPv4 mcast routes (mroutes)	4000	4000	4000
IPv6 mcast routes (mroutes)	1000	1000	1000

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
Bridge Domains	4094	4094	4094
EoMPLS Tunnels	4000	4000	4000
MPLS VPN	1000	1000	1000
VRF Lite	1000	1000	1000
VPLS Instances[3]	3500	3500	3500
IPv4 ACL entries	1000 (984 user configurable)	1000 (984 user configurable)	1000 (984 user configurable)
IPv6 ACL entries	128 (124 user configurable)	128 (124 user configurable)	128 (124 user configurable)
v4 QOS Classifications	16000	16000	16000
v6 QoS Classifications	NS	NS	NS
Egress policers per ASIC	NS	NS	NS
OAM sessions	1000	1000	1000
IPSLA sessions	1000	1000	1000
EFP	16000	16000	16000
Maximum VLANs per port	4,000 per ASIC	4,000 per ASIC	4,000 per ASIC
Maximum VPLS neighbors	64	64	64
Maximum attachment circuit per BD	64	64	64
STP Instances	16	16	16
Maximum Etherchannel groups	48	48	48
Maximum Interfaces per Etherchannel groups	8	8	8
Maximum VRRP per system	255	255	255
Maximum HSRP per system	255	255	255
Maximum Ingress MPLS labels	32000	32000	32000

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
Maximum FRR/TE Headend	500	500	500
Maximum FRR/TE Midpoints	5000	5000	5000
Maximum E-LMI sessions	128	128	128
Maximum BFD sessions	1023	1023	1023
Maximum SPAN/RSPAN sessions	10	10	10
Maximum Queue counters per ASIC/system	40000/48000	40000/48000	40000/48000
Maximum Policer counters per ASIC/system	12000/24000	12000/24000	12000/24000
Max BDI for L3	1000	1000	1000
Multicast OIF per group for VF Lite or mVPN	255	255	255
Multicast OIF per group for native multicast	255	255	255
Queues per ASIC/system	40000/48000	40000/48000	40000/48000
Max Queues per EFP	8	8	8
Ingress Classifications	16000	16000	16000
Egress Classifications	48000	48000	48000
Max Ingress Policers per ASIC/system	12000/24000	12000/24000	12000/24000
Max Egress Policers per ASIC/system	NS	NS	NS
Maximum EFPs per BD	256	256	256
Maximum number of BDI for PW	128	128	128
Maximum Layer 3 interfaces	1000	1000	1000
Max REP segments	NS	NS	NS
Maximum class-maps	1000	1000	1000

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
Maximum policy maps	1000	1000	1000
Max number of OSPF Neighbors	400	400	400
Max number of ISIS neighbors	400	400	400
Max number of ISIS instances	30	30	30
Max number of BGP neighbors	250	250	250
Max number IEEE 802.1ag/Y.1731(CFM) instances at 1sec for xconnect	1000	1000	1000
Max number IEEE 802.1ag/Y.1731(CFM) instances at 3.3 ms for BD & xconenct	1000	1000	1000
Max number IEEE 802.1ag/Y.1731(CFM) instances at 100 ms for BD & xconnect	1000	1000	1000
Max number IEEE 802.1ag/Y.1731(CFM) instances at 1Sec for BD	1000	1000	1000
Max number of Y.1731 instances	1000	1000	1000
Maximum Class-maps in policy-map	512	512	512
Max number of match statements per class-map	16	16	16
Max number of BFD sessions at 3.3ms	1023	1023	1023
Max number of BFD sessions at 100ms	1023	1023	1023
Max number of BFD sessions at 1S	1023	1023	1023

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
Max number of IGP Prefixes protected via LFA-FRR	1500	1500	1500
Max number of L3VPN Prefixes protected via LFA-FRR	4000	4000	4000
Max number of L2VPN sessions protected via LFA-FRR	2000	2000	2000

[3] From release 16.7.x the VPLS backup PW feature is supported, so if VPLS instance is configured then the maximum VPLS session is limited to 1000 instead of 3500.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP2.

Table 26: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP2)

Resource	Default Template	Video Template	IP Template	Maximum IPv6 QoS Template
MAC table	16000	16000	16000	16000
Virtual local area network (VLAN) mapping	4000	4000	65536	4000
IPv4 routes[4]	20000	12000	24000	20000
IPv6 routes	3962	3962	1914	3962
VPNv4 routes[5]	20000	12000	24000	20000
VPNv6 routes	3962	3962	1914	3962
IPv4 multicast routes (mroutes)	1000	2000	1000	1000
Layer 2 multicast groups[6]	NA	NA	NA	NA
Bridge Domains (BD)	4000	4000	4000	4000
MAC-in-MAC	0	0	0	0
Ethernet over MPLS (EoMPLS) tunnels	2000	2000	2000	2000

Resource	Default Template	Video Template	IP Template	Maximum IPv6 QoS Template
MPLS Virtual Private Network (VPN)	128	128	128	128
Virtual Routing and Forwarding (VRF) lite	128	128	128	128
Virtual Private LAN Services (VPLS) instances	2000	2000	2000	2000
Access Control List (ACL) entries[7]	2000	4000	2000	2000
Queues per Application-Specific Integrated Circuit (ASIC) [8]	4095	4095	4095	4095
IPv4 Quality of Service (QoS) classifications	4096	2048	4096	4096
Policers	4096	4096	4096	4096
Ethernet Operations, Administration, and Maintenance (OAM) sessions	1000	1000	1000	0
IP Service Level Agreements (IPSLA) sessions	1000	1000	1000	1000
Ethernet Flow Point (EFP)	8000	8000	8000	8000
Maximum VLANs per port	4094	4094	4094	4094
Maximum I-TAG per system	500	500	500	500
Maximum VPLS neighbors	64	64	64	64
Maximum attachment circuit per BD	128	128	128	128
STP Instances	16	16	16	16

Resource	Default Template	Video Template	IP Template	Maximum IPv6 QoS Template
Maximum Etherchannel groups	64	64	64	64
Maximum Interfaces per Etherchannel groups	8	8	8	8
Maximum Hot Standby Router Protocol (HSRP)	128 (For Cisco IOS-XE Release 3.14 and earlier) 256 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 256 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 256 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 256 (For Cisco IOS-XE Release 3.15 and later)
Maximum Virtual Router Redundancy Protocol (VRRP)	128 (For Cisco IOS-XE Release 3.14 and earlier) 255 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 255 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 255 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 255 (For Cisco IOS-XE Release 3.15 and later)
Maximum Ingress MPLS labels	32000	32000	32000	32000
Maximum Egress MPLS labels	28500	28500	28500	28500
Maximum Fast Reroute (FRR)/Traffic Engineering (TE) headend	500	500	500	500
Maximum FRR/TE midpoints	5000	5000	5000	5000
Maximum Enhanced Local Management Interface (E-LMI) sessions	1000	1000	1000	1000
Maximum Bidirectional Forwarding Detection (BFD) sessions	1023	1023	1023	1023

Resource	Default Template	Video Template	IP Template	Maximum IPv6 QoS Template
Maximum Switched Port Analyzer (SPAN)/Remote SPAN (RSPAN) sessions	32	32	32	32
Maximum Queue counters (packet & byte)	65536	65536	65536	65536
Maximum Policer counters (packet & byte)	49152	49152	49152	49152
Maximum number of BDI for Layer 3	1000	1000	1000	1000
IPv6 ACL	1000	1000	1000	2000
IPv6 QoS classification	4096	4096	4096	4096
Maximum Number of Layer 4 Source/Destination matches per interface [9]	8	8	8	NA

[4] Using IPv4 and VPNv4 routes concurrently reduces the maximum scaled value as both the routes use the same TCAM space.

[5] Due to label space limitation of 16000 VPNv4 routes, to achieve 24000 VPNv4 routes in IP template use per VRF mode.

[6] Using Layer 2 and Layer 3 multicast groups concurrently reduces the scale number to 1947.

[7] ACLs contend for TCAM resources with Multicast Virtual Private Network (MVPN).

[8] User available queues are 1920.

[9] TCAM consumption for IPv6 Qos ACL Layer 4 port match operations increase with Maximum IPv6 Qos SDM template.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP1A.

Table 27: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP1A)

Resource	IP template	Video template
MAC table	16000	16000
Virtual local area network (VLAN) mapping	4000	4000
IPv4 routes[10]	24000	12000

Resource	IP template	Video template
IPv6 routes[11]	4000	4000
VPNv4 routes[12]	24000	12000
VPNv6 routes	4000	4000
IPv4 multicast routes (mroutes)	1000	2000
Layer 2 multicast groups[13]	1000	2000
Bridge Domains (BD)	4094	4094
MAC-in-MAC	0	0
Ethernet over MPLS (EoMPLS) tunnels	512	512
MPLS Virtual Private Network (VPN)	128	128
Virtual Routing and Forwarding (VRF) lite	128	128
Virtual Private LAN Services (VPLS) instances	26	26
Access Control List (ACL) entries[14]	2000	4000
Queues per Application-Specific Integrated Circuit (ASIC) [15]	2048	2048
IPv4 Quality of Service (QoS) classifications	4096	2048
Policers	1024	1024
Ethernet Operations, Administration, and Maintenance (OAM) sessions	1000	1000
IP Service Level Agreements (IPSLA) sessions	1000	1000
Ethernet Flow Point (EFP)	4000	4000
Maximum VLANs per port	4094	4094
Maximum I-TAG per system	500	500
Maximum VPLS neighbors	62	62
Maximum attachment circuit per BD	62	62
STP Instances	16	16
Maximum Etherchannel groups	26	26

Resource	IP template	Video template
Maximum Interfaces per Etherchannel groups	8	8
Maximum Hot Standby Router Protocol (HSRP)/Virtual Router Redundancy Protocol (VRRP)	128	128
Maximum Ingress MPLS labels	16000	16000
Maximum Egress MPLS labels	28500	28500
Maximum Fast Reroute (FRR)/Traffic Engineering (TE) headend	512	512
Maximum FRR/TE midpoints	5000	5000
Maximum Enhanced Local Management Interface (E-LMI) sessions	1000	1000
Maximum Bidirectional Forwarding Detection (BFD) sessions	511	511
Maximum Switched Port Analyzer (SPAN)/Remote SPAN (RSPAN) sessions	32	32
Maximum Queue counters (packet & byte)	65536	65536
Maximum Policer counters (packet & byte)	49152	49152
Maximum number of BDI for Layer 3	256	256
IPv6 ACL	1000	1000
IPv6 QoS classification	4096	2048

[10] Using IPv4 and VPNv4 routes concurrently reduces the maximum scaled value as both the routes use the same TCAM space.
[11] User available routes are 3967.
[12] Due to label space limitation of 16000 VPNv4 routes, to achieve 24000 VPNv4 routes in IP template use per VRF mode.
[13] Using Layer 2 and Layer 3 multicast groups concurrently reduces the scale number to 1947.
[14] ACLs contend for TCAM resources with Multicast Virtual Private Network (MVPN).
[15] User available queues are 1920.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP1B.

Table 28: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP1B)

Resource	VPNv4/v6 template	Video template
MAC table	256000	256000
IVLAN mapping	4000	4000
EVLAN mapping	4000	4000
Maximum VLANS per port	4094	4094
Maximum security addresses per EFP	1000	1000
Maximum security addresses per BD	10000	10000
Maximum security addresses	256000	256000
Maximum security configuration addresses	256000	256000
EFPs per BD	62	62
IPv4 routes	80000	80000
IPv6 routes	40000	8000
Maximum BD interfaces	1000	1000
Maximum ITAG per system	500	500
IPv4 routing groups[16]	2000	8000
IPv6 routing groups[17]	2000	8000
IPv4 multicast groups[18]	2000	10000
IPv6 multicast groups[19]	2000	10000
BDs	4000	4000
MAC-in-MAC	0	0
EoMPLS tunnels	8000	8000
MPLS VPN	1000	1000
Virtual Routing and Forwarding Scale (VRFS)	1000	1000
VPLS instances	2000	2000
Maximum VPLS neighbors	62	62
ACL entries	4000	4000
IPv6 ACL entries	1000	1000
Queues per ASIC	16384	16384
Classifications	12288	12288
Ingress policers per ASIC	8192	8192

Resource	VPNv4/v6 template	Video template
Egress policers per ASIC	4096	4096
Maximum class maps	4096	4096
Maximum policy maps	1024	1024
Maximum queue counters	65536	65536
Maximum policer counters	48152	48152
OAM sessions	4000	4000
ELMI sessions	1000	1000
SLA sessions	1000	1000
EFPs	8000	8000
MPLS ingress labels	64000	64000
MPLS egress labels	80000	80000
FRR TE headend	1000	1000
FRR TE midpoints	7000	7000
STP instances	128	128
BFD sessions	511	511
HSRP VRRP sessions	256	256
Maximum EC groups	16	16
Maximum interfaces per EC groups	8	8
Maximum SPAN RSPAN sessions	32	32
IPv4 tunnel entries	1000	1000
Maximum VPNv4 and VPNv6 pre-fixes[20]	64000	64000

[16] Overall multicast groups in video template can be scaled to 8000 individually or in combination with other multicast features. For example: IPv4 routing groups can be scaled to 8000 or IPv4 routing groups and IPv6 routing groups together can be scaled to 8000.

[17] See footnote 7.

[18] See footnote 7.

[19] See footnote 7.

[20] VPNv4 and VPNv6 together can be scaled up to 64000 in per-prefix mode.

Selecting the SDM Template

To select an SDM template, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**sdm prefer** {**default** | **video** | **ip** | **mvpn_rsp1a** | **VPNv4/v6** | **max-ipv6-acl** | **enable_4x_priority** | **enable_copp** | **enable_acl_copp** | **ipv4** | **ipv6** | **efp_feat_ext** | **enable_8k_efp** | | **enable_bdi_mtu** | **enable_copp** | **enable_l3vpn_cm** | **enable_color_blind_policer** | **enable_l3vpn_cm** | **enable_match_inner_dscp** | **enable_portchannel_qos_multiple_active** | **vpls_stats_enable** | **enable_dhcp_snoop** | **enable_hitless_switching** | **enable_l2pt_fwd_all** | **enable_l3vpn_cm** | **enable_latching_loopback** | **enable_multicast_stats** | **enable_qos_scale** | **enable_tdm_to_ip_iw** | **enable_vlan_translation** | **ipv4ipv4_ipv6** | **ipv6** | **no_efp_feat_ext** | **sr_5_label_push_enable** | **sr_pfp_enable**}
	Example:
	`Router(config)# sdm prefer default`
		Specifies the SDM template to be used on the router.
		- default—Balances all functions.
		- video—Increases multicast routes and ACLs.
		- mvpn_rsp1a—Supports MVPN. This option is available only on RSP1A.
		- VPNv4/v6—Increases IPv4/VPNv4 routes. This option is available only on RSP1B.
		- max-ipv6-acl—Supports IPv6 QoS ACL routes. The NEQ Layer 4 operation is supported in maximum IPv6 QoS ACL template.
		- ipv4—Enables the IPv4 template. This is supported on the RSP3 module.
		- ipv6—Enables the IPv6 feature template. This is supported on the RSP3 module.
		- efp_feat_ext—Enables the EFP feature template. This is supported on the RSP3 module.
		- enable_8k_efp—Enables the 8K EFP feature template. This is supported on the RSP3 module.
		- enable_bdi_mtu—Enables the BDI MTU feature template. This is supported on the RSP3 module.
		- enable_4x_priority—Enables the 4x Priority feature template. This is supported on the RSP3 module.
		- enable_copp—Enables the COPP feature template. This is supported on the RSP3 module.

	Command or Action	Purpose
		• enable_acl_copp—Enables the COPP ACL feature template. This is supported on the RSP3 module. • enable_l3vpn_cm—Enables the L3VPN conditional marking feature template. This is supported on the RSP3 module. • enable_color_blind_policer—Enables the Color Blind Policer feature template. This is supported on the RSP3 module. • enable_match_inner_dscp—Enables the match inner dscp feature template. This is supported on the RSP3 module. • enable_portchannel_qos_multiple_active—Enables the port channel QoS multiple active feature template. This is supported on the RSP3 module. • vpls_stats_enable—Enables the VPLS statistics feature template. This is supported on the RSP3 module. • enable_dhcp_snoop—Allows the DHCP traffic which ingress on the cross-connect service instance to be forwarded in the data plane, whereas the Bridge Domain (BD) service instance frames should be trapped to CPU to support the DHCP Option 82. • enable_hitless_switching—Enables the Hitless Switching feature template. This is supported on the RSP3 module. • enable_l2pt_fwd_all—Enables the L2PT forward All feature template. This is supported on the RSP3 module. • enable_l3vpn_cm—Enables the L3VPN CM feature template. This is supported on the RSP3 module. • enable_latching_loopback—Enables the Latching Loopback feature template. This is supported on the RSP3 module. • enable_multicast_stats —Enables the Multicast Stats feature template. This is supported on the RSP3 module.

	Command or Action	Purpose
		• enable_qps_scale—Enables the Qos Scale feature template. This is supported on the RSP3 module. • enable_tdm_to_ip_iw—Enables the TDM to IP IW feature template. This is supported on the RSP3 module. • enable_vlan_translation—Enables the VLAN Translation feature template. This is supported on the RSP3 module. • ipv4—Enables the IPv4 feature template. This is supported on the RSP3 module. • ipv4_ipv6—Enables the IPv4_IPv6 feature template. This is supported on the RSP3 module • ipv6—Enables the IPv6 feature template. This is supported on the RSP3 module. • no_efp_feat_ext—Enables the No EFP FEAT EXT feature template. This is supported on the RSP3 module. • sr_5_label_push_enable —Enables the SR 5 labels Push feature template. This is supported on the RSP3 module. • sr_pfp_enable—Enables the SR PFP feature template. This is supported on the RSP3 module. **Note** When changing the SDM template, the router waits for two minutes before reloading. Do not perform any operation till the router reloads. **Note** For the new SDM template to take effect, you must save and reload the new configuration, otherwise the current SDM template is retained. **Note** For more information, see Supported SDM Template.
Step 4	**sdm prefer enable_vlan_translation** **Example:** `sdm prefer enable_vlan_translation`	Enables VLAN Translation on the Cisco RSP3 module.

	Command or Action	Purpose

	`Router(config)#sdm prefer`
	`enable_vlan_translation`
	`Standby is reloaded, it will come up with`
	` init required for new template`
	`once standby comes up`
	`Please trigger SSO`
	`Changes to VLAN Translation template`
	`stored`	

Step 5	**sdm prefer disable_vlan_translation**
	Example:
	`sdm prefer disable_vlan_translation`
	
	`Router(config)#sdm prefer`
	`disable_vlan_translation`
	`Standby is reloaded, it will come up with`
	` init required for new template`
	`once standby comes up`
	`Please trigger SSO`
	`Changes to VLAN Translation template`
	`stored`
		Disables VLAN Translation on the Cisco RSP3 module.

Verifying the SDM Template

You can use the following **show** commands to verify configuration of your SDM template:

- **show sdm prefer**—Displays the resource numbers supported by the specified SDM template.

SDM Template Supported Features on RSP3 Module

This section details the supported SDM template features on the RSP3 module. The sdm prefer command provides the follwing templates:

Table 29: SDM Templates and Supported Features

SDM Template	Supported Feature
sdm prefer vpls_stats_enable	VPLS Statistics
sdm prefer efp_feat_ext	Split-Horizon Groups
sdm prefer enable_8k_efp	8K EFP (4 Queue Model)
sdm prefer enable_match_inner_dscp	Match Inner DSCP
sdm prefer enable_copp	Control Plane Policing
sdm prefer enable_portchannel_qos_multiple_active	QoS Support on Port Channel LACP Active Active 16K EFP Support on Port Channel

SDM Template	Supported Feature
sdm prefer ipv4_ipv6	Enhance uRPF scale to 32K
sdm prefer enable_vlan_translation	VLAN Translation for RSP3
sdm prefer enable_hitless_switching	Hitless Switching on C37.94 Interface Module

VPLS Statistics

VPLS statistic feature supports packet and byte count in ingress and egress directions. The following are the required criteria to enable this feature:

- Metro Aggregation services license
- Special SDM template

  Use the following commands to enable or disable VPLS statistics feature:

  ```
  sdm prefer vpls_stats_enable
  sdm prefer vpls_stats_disable
  ```

After template configuration, the node is auto reloaded.

Restrictions

- EFP statistics is not supported when VPLS statistics is enabled.
- Transit packet drops data is not supported.
- There is a sync time of 10 seconds between the software and the hardware for fetching the statistics.
- If access rewrite is configured (pop 1), VC statistics show 4 bytes less than the actual size (in both imposition and disposition node) because pop 1 removes the VLAN header.
- VC statistics do not account LDP and VC label. It displays what is received from access in both imposition and disposition node.

Example

The following example shows a sample VPLS Statics counter output:

```
router#show mpls l2transport vc 2200 detail

Local interface: Gi0/14/2 up, line protocol up, Ethernet:100 up
  Destination address: 10.163.123.218, VC ID: 2200, VC status: up
    Output interface: Te0/7/2, imposed label stack {24022 24025}
    Preferred path: not configured
    Default path: active
    Next hop: 10.163.122.74
  Create time: 20:31:49, last status change time: 16:27:32
    Last label FSM state change time: 16:27:44
  Signaling protocol: LDP, peer 10.163.123.218:0 up
    Targeted Hello: 10.163.123.215(LDP Id) -> 10.163.123.218, LDP is UP
    Graceful restart: configured and enabled
    Non stop routing: configured and enabled
    Status TLV support (local/remote)    : enabled/supported
      LDP route watch                    : enabled
      Label/status state machine         : established, LruRru
      Last local dataplane   status rcvd: No fault
```

```
    Last BFD dataplane     status rcvd: Not sent
    Last BFD peer monitor  status rcvd: No fault
    Last local AC  circuit status rcvd: No fault
    Last local AC  circuit status sent: No fault
    Last local PW i/f circ status rcvd: No fault
    Last local LDP TLV     status sent: No fault
   Last remote LDP TLV    status rcvd: No fault
    Last remote LDP ADJ    status rcvd: No fault
  MPLS VC labels: local 110, remote 24025
  Group ID: local 40, remote 67109248
  MTU: local 9000, remote 9000
  Remote interface description: TenGigE0_0_2_3.2200
Sequencing: receive disabled, send disabled
Control Word: Off (configured: autosense)
SSO Descriptor: 10.163.123.218/2200, local label: 110
Dataplane:
  SSM segment/switch IDs: 16911/90633 (used), PWID: 71
VC statistics:
  transit packet totals: receive 100, send 200
  transit byte totals:   receive 12800, send 25600
  transit packet drops:  receive 0, seq error 0, send 0
```

Split Horizon Enhancements on the RSP3 Module

Starting with Cisco IOS XE Release 16.6.1, the **efp_feat_ext** template is introduced. This template when enabled allows configuration of two split-horizon groups on the EVC bridge-domain.

- Two Split-horizon groups—Group 0 and Group 1 are configured through using the **bridge-domain** *bd number* **split-horizon group** *0-1* command.

Prerequisites for Split-Horizon Groups on the RSP3 Module

- The efp_feat_ext template must be configured to enable the feature.
- Metro services license must be enabled; LICENSE_ACTIVE_LEVEL=metroaggrservices,all:ASR-903;

Restrictions for Split-Horizon Groups on the RSP3 Module

- If a VPLS VFI is part of the bridge-domain configuration, the VPLS is by default part of Split-horizon group 0 and the scale for Split-horizon group 1-2 and No group is applicable as in the Table 2.
- The overall scale of EFPs is 8K, only if the split-horizon groups are configured. For information, see supported scale.

Note If split-horizon based-EFPs aren’t configured, the total EFPs supported are 4K.

- EFPs configured on the same bridge domain and same split-horizon group, can’t forward to or receive traffic from each other.
- We don’t recommended configuration of Y.1564 and split-horizon group on the same EFP.
- We don’t recommend configuring MAC security with split-horizon group.

- Split-horizon group isn’t supported for CFM on this template. Configuring split-horizon groups on CFM-based MEPs may result in MEPs being unlearned, and unexpected behavior may be observed.
- If ethernet loopback is configured, and if a dynamic change in split-horizon group occurs on the EFP-BD, the ELB session must be restarted.
- A change in the split-horizon group configuration on a regular EFP results in hardware programming update and may impact L2 traffic. This results in a MAC-flush and relearn of traffic with new MAC address.

Following are known behavior of split-horizon groups:

- Changing the split-horizon group on any EFP, results in traffic flooding back to same EFP for few milliseconds.
- A small traffic leak may be observed on defaulting an interface with higher number of EFP with split-horizon configured.
- BFD flaps and underlying IGP flaps may be observed upon changing split-horizon groups, if BFD is hardware-based.

Split-Horizon Supported Scale

8K EFPs are supported across RSP3-400 and 4K EFPs on RSP3-200.

Note If Split-horizon configuration does not exist, number of EFPs supported are reduced to 4K EFPs.

Table 30: Split-Horizon Supported Template

Split-Horizon Group	RSP3-400	RSP3-200
Default (No config)	4K EFP	2K EFP
Group 0	2K EFP	1K EFP
Group 1	2K EFP	1K EFP

Note Port-channel scale is half the regular scale of the EFP.

Configuring Split-Horizon Group on the RSP3 Module

```
interface GigabitEthernet0/2/2
service instance 1 ethernet
  encapsulation dot1q 100
  bridge-domain 100 split-horizon group 0   When you configure split-horizon group 0,(0
is optional)

 interface GigabitEthernet0/2/2
service instance 2 ethernet
```

```
encapsulation dot1q 102
bridge-domain 102 split-horizon group 1  When you configure split-horizon group 1
```

8K EFP (4 Queue Model)

In Cisco IOS XE Release 3.18SP, the 8K EFP (4 Queue Model) support allows up to 8000 EFPs at the system level. EFP scale implementation follows the static model, that is, eight queues are created per EFP by default.

Information About 8000 (8K) EFP

- In default model, 5000 EFPs can be configured on Cisco NCS 4200 RSP3 module.
- The Switch Database Management (SDM) template feature can be used to configure 8000 EFPs across ASIC(4000 EFPs per ASIC interfaces).
- In 8K EFP model, each EFP consumes four Egress queues. If 8K EFP SDM template is not enabled, each EFP consumes eight Egress queues.
- Ingress policy map can specify more than eight traffic classes based on PHB matches, which remains the same. However, Egress policy map can have three user defined class and class-default class.
- Each Egress class-maps can be mapped to a single or multiple traffic classes and each class-map mapped to a single queue.
- Maximum of two queues are set to Priority according to policy configuration.
- All the existing QOS restrictions that apply in default model are also applicable to 8K EFP model.

Prerequisites for 8000 (8K) EFP

- Activate the Metro Aggregation Services license on the device.
- To configure 8000 EFPs, enable the SDM template using CLI **sdm prefer enable_8k_efp**.
- Reset the SDM template using the CLI **sdm prefer disable_8k_efp** .

Restrictions for 8000 (8K) EFP

- With the **enable_8k_efp** SDM template, shut or noshut on Port-channel (PoCH) is blocked. To make the PoCH as UP or DOWN, all the port channel member links must be either shut or noshut.
- Traffic class to Queue mapping is done per interface and not per EVC.
- Four traffic classes including class-default can be supported in Egress policy.
- Same three traffic classes or subset of three traffic classes match is supported on EVCs of an interface.
- Traffic classes to queue mapping profiles are limited to four in global, hence excluding class-default, only three mode unique combinations can be supported across interfaces.
- TRTCM always operates with conform-action transmit, exceed-action transmit and violate-action drop.
- By default, 1R2C Policer will behave as 1R3C Policer in 4 Queue model.
- All the QOS restrictions that is applicable in default mode is also applicable in 8k EFP mode

Configuring 8K Model

Configuring 8K EFP Template

Below is the sample configuration to enable 8K EFP or 4 Queue mode template. On enabling **sdm prefer enable_8k_efp**, the router reloads and boots up with 8K EFP template.

```
RSP3-903(config)#sdm prefer enable_8k_efp

Template configuration has been modified. Save config and Reload? [yes/no]: yes
Building configuration...

Jul 22 05:58:30.774 IST: Changes to the EFP template preferences have been stored[OK]
Proceeding with system reload...
Reload scheduled for 06:00:38 IST Fri Jul 22 2016 (in 2 minutes) by console
Reload reason: EFP template change
```

Verifying 8K EFP Template

You can verify the current template as below.

```
Device#sh sdm prefer current

The current sdm template is "default" template and efp template is "enable_8k_efp" template
```

Configuring QOS in 8K EFP Model

Below is sample configuration to configure egress policy map when 4Q mode is enabled.

```
Device#enable
Device#configure terminal
Device(config)#interface GigabitEthernet0/3/0
Device(config-if)#service instance 10 e
Device(config-if-srv)#service-policy output egress



Current configuration : 193 bytes
!
policy-map egress
class qos2
  shape average 2000000
 class qos3
  shape average 3000000
 class qos4
  shape average 4000000
 class class-default
  shape average 5000000
!
end
```

```
Device#sh run class-map qos2
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos2
match qos-group 2
!
end
```

```
Device#sh run class-map qos3
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos3
match qos-group 3
!
end


Device#sh run class-map qos4
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos4
match qos-group 4
!
end
```

Verifying QOS in 8K EFP Model

You need to verify the interface and policy-map details to check 8K model queue is working.

```
Device# show run interface g0/3/0
Building configuration...

Current configuration : 217 bytes
!
interface GigabitEthernet0/3/0
no ip address
negotiation auto
service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  service-policy output egress
  bridge-domain 10
!
end
```

```
Router#show running-config policy-map egress
Building configuration...

Current configuration : 193 bytes
!
policy-map egress
class qos2
shape average 2000000
class qos3
shape average 3000000
class qos4
shape average 4000000
class class-default
shape average 5000000
!
end
```

```
Device#sh policy-map int g0/3/0 serv inst 10
Port-channel10: EFP 10

Service-policy output: egress

Class-map: qos2 (match-all)
```

```
122566 packets, 125262452 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 2
Queueing
queue limit 4096000 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/119746/0
(pkts output/bytes output) 2820/2882040
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000

Class-map: qos3 (match-all)
122566 packets, 125262452 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 3
Queueing
queue limit 2730666 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/118806/0
(pkts output/bytes output) 3760/3842720
shape (average) cir 3000000, bc 12000, be 12000
target shape rate 3000000

Class-map: qos4 (match-all)
245131 packets, 250523882 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 4
Queueing
queue limit 2048000 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/239961/0
(pkts output/bytes output) 5170/5283740
shape (average) cir 4000000, bc 16000, be 16000
target shape rate 4000000

Class-map: class-default (match-any)
245131 packets, 250523882 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 1638400 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/239961/0
(pkts output/bytes output) 5170/5283740
shape (average) cir 5000000, bc 20000, be 20000
target shape rate 5000000
Device#
```

16K EFP Support on Port Channel

Starting with Cisco IOS XE 16.8.1 release, 16K EFPs on port channel are supported on the RSP3 module.

The following are the key features supported:

- In order to enable 16K EFP over a port channel, you need to enable the following template:

  enable_portchannel_qos_multiple_active

- 16000 EFPs are supported on the RSP3 module (8K EFPs are supported per ASIC). Each port can have a maximum of 8K EFPs configured.
- 8K bridge domains are supported.
- On the RSP3 module, 1024 BDI interfaces that include physical interface, port channel interface, and BDI are available, and these interfaces can be configured upto 4096 BDI interfaces.

Note

- If a port channel is configured on an application-specific integrated circuit (ASIC), for example ASIC 0 , then ensure that physical members to be added to port channel also should be in the same ASIC.
- While adding member links to port channels with 3K to 8K EFPs, the router sends CPUHOG messages to the console output to inform that this process has consumed CPU memory. The number of messages increases with the increase in the scale of the EFPs. Such messages do not impact any functionality. They ensure that the system does not become unresponsive or locked up due to the total consumption of the CPU.

Restrictions for 16K EFP on Port Channel

- G.8032, SADT, CFM, and TEFP are not supported on the port channel.
- 16k EFP scale is not supported if SDM template is enabled for split horizon scale.
- Minimal traffic outage (for example, in milliseconds) is observed, when a policy map is applied or removed.
- In a complete scale environment, the EFP statistics update requires more than 1 minute to complete.

Configuring 16K EFP on Port Channel

To configure 16K EFP on port channel, use the following commands:

```
router>enable
router#configure terminal
router(config)#sdm prefer enable_portchannel_qos_multiple_active
router(config)#platform port-channel 10 members-asic-id 1
router(config)#platform qos-port-channel_multiple_active port-channel 10
router(config)#interface port-channel 10
router(config-if)#end
```

After the SDM template update, the device reloads automatically and you need to enter *yes* to save the configuration.

Verifying 16k EFP on Port Channel

The following are examples to verify for 16K EFP configuration on port channel.

show etherchannel summary

```
Router# show etherchannel summary
Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
```

```
10      Po10(RU)                LACP     Te0/5/0(bndl) Te0/5/1(bndl)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

show ethernet service instance id interface stats

```
Router# show ethernet service instance id 12000 interface port-channel 10 stats
Port maximum number of service instances: 16000
Service Instance 12000, Interface port-channel 10
   Pkts In   Bytes In   Pkts Out  Bytes Out
       252     359352        252     359352
```

show ethernet service instance summary

```
Router# show ethernet service instance summary
System summary
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain     16000    16000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all         16000    16000        0        0        0        0        0        0
Associated interface: port-channel 10
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
Associated interface: port-channel 11
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
```

Control Plane Policing

The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOSCisco IOS XE routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Restrictions for Control Plane Policing

Input Rate-Limiting Support

Input rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to input control plane traffic with the **service-policy input** command. For more information, see the “Input Rate-Limiting and Silent Mode Operation” section.

MQC Restrictions

The Control Plane Policing feature requires the Modular QoS CLI (MQC) to configure packet classification and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing.

Match Criteria Support

Only the extended IP access control lists (ACLs) classification (match) criteria is supported.

Restrictions for CoPP

- IPv6 is not supported.
- Port range ACL is not supported.
- Due to hardware limitation, to match the control plane packets against CoPP, ACL rules that match with IP addresses should be added, since adding generic ACL rules with any any matches both the data plane and control plane traffic.

Restrictions for CoPP on the RSP3

- CoPP does not support multi match. ACLs with DSCP and fragment option enabled does not filter or classify packets under CoPP.
- Effective Cisco IOS XE Bengaluru 17.5.1 **enable_copp_copp** and **enable_acl** template must be configured on the RSP3 module to activate CoPP.
- Ingress and Egress marking are not supported.
- Egress CoPP is not supported. CoPP with marking is not supported.
- CPU bound traffic (punted traffic) flows is supported via the same queue with or without CoPP.
- Only match on access group is supported on a CoPP policy.
- Hierarchical policy is not supported with CoPP.
- Class-default is not supported on CoPP policy.
- User-defined ACLs are not subjected to CoPP classified traffic.
- A CoPP policy map applied on a physical interface is functional.
- When CoPP template is enabled, classification on outer VLAN, inner VLAN, Inner VLAN Cos, destination MAC address, source IP address, and destination IP address are not supported.

  The template-based model is used to enable CoPP features and disable some of the above mentioned QoS classifications.
- When **enable_acl_copp** template is enabled, **sdm prefer enable_match_inner_dscp** template is not supported.
- Only IP ACLs based class-maps are supported. MAC ACLs are not supported.
- Multicast protocols like PIM and IGMP are not supported.
- Only CPU destined Unicast Layer3 protocols packets are matched as part of CoPP classification.

- Do not configure CoPP and BDI-MTU SDM templates together, as it is not supported.
- Management packets cannot be filtered based on source TCP/UDP Ports and destination IP address.
- Ensure to enable the CoPP Version 2 template to enable the CoPP feature.
- Two ACL entries will be added for IPV4 and L3VPN cases for each ACL entry in the configuration.

Restrictions on Firmware

- Port ranges are not supported.
- Only exact matches are supported, greater than, less than and not equal are not supported.
- Internet Control Message Protocol (ICMP) inner type's classification not supported.
- Match any is only supported at a class-map level.
- Policing action is supported on a CoPP policy map.

Supported Protocols

The following table lists the protocols supported on Control Plane Policing feature. It is mandatory that the IP address should match the source or destination IP address.

Table 31: Supported Protocols

Supported Protocols	Criteria	Match	Queue#
TFTP - Trivial FTP	Port Match	IP access list ext copp-system-acl-tftp permit udp any any eq 69	NQ_CPU_HOST_Q
TELNET	Port Match	IP access list ext copp-system-acl-telnet permit tcp any any eq telnet	NQ_CPU_CONTROL_Q
NTP - Network Time Protocol	Port Match	IP access list ext copp-system-acl-ntp permit udp any any eq ntp	NQ_CPU_HOST_Q
FTP - File Transfer Protocol	Port Match	IP access list ext copp-system-acl-ftp permit tcp host any any eq ftp	NQ_CPU_HOST_Q
SNMP - Simple Network Management Protocol	Port Match	IP access list ext copp-system-acl-snmp permit udp any any eq snmp	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
TACACS - Terminal Access Controller Access-Control System	Port Match	IP access list ext copp-system-acl-tacacs permit tcp any any tacacs	NQ_CPU_HOST_Q
FTP-DATA	Port Match	IP access list ext copp-system-acl-ftpdata permit tcp any any eq 20	NQ_CPU_HOST_Q
HTTP - Hypertext Transfer Protocol	Port Match	IP access list ext copp-system-acl-http permit tcp any any eq www	NQ_CPU_HOST_Q
WCCP - Web Cache Communication Protocol	Port Match	IP access list ext copp-system-acl-wccp permit udp any eq 2048 any eq 2048	NQ_CPU_HOST_Q
SSH - Secure Shell	Port Match	IP access list ext copp-system-acl-ssh permit tcp any any eq 22	NQ_CPU_HOST_Q
ICMP - Internet Control Message Protocol	Protocol Match	IP access list copp-system-acl-icmp permit icmp any any	NQ_CPU_HOST_Q
DHCP - Dynamic Host Configuration Protocol	Port Match	IP access list copp-system-acl-dhcp permit udp any any eq bootps	NQ_CPU_HOST_Q
MPLS- OAM	Port Match	IP access list copp-system-acl-mplsoam permit udp any eq 3503 any	NQ_CPU_HOST_Q
LDP - Label Distribution Protocol	Port Match	IP access list copp-system-acl-ldp permit udp any eq 646 any eq 646 permit tcp any any eq 646	NQ_CPU_CFM_Q

Supported Protocols	Criteria	Match	Queue#
RADIUS - Remote Authentication Dial In User Service	Port Match	IP access list copp-system-radius permit udp any any eq 1812 permit udp any any eq 1813 permit udp any any eq 1645 permit udp any any eq 1646 permit udp any eq 1812 any permit udp any eq 1813 any permit udp any eq 1645 any	NQ_CPU_HOST_Q
Network Configuration Protocol (NETCONF)	IP/Port Match	IP access list ext copp-system-acl-telnet permit tcp any any eq 830 - NETCONF	NQ_CPU_HOST_Q
PostgreSQL Support	IP/Port Match	IP access list ext copp-system-acl-telnet PostgreSQL IP/Port Match permit tcp 169.223.252.0.0 0.0.3.255 host 169.223.253.1 eq 5432	NQ_CPU_HOST_Q
Source IP or Destination IP	IP/Port Match	Permit IP host 10.1.1.1 or 10.1.1.2 **Note** The **`permit ip any any`** command is not supported.	NQ_CPU_HOST_Q

Input Rate-Limiting and Silent Mode Operation

A router is automatically enabled to silently discard packets when you configure input policing on control plane traffic using the **service-policy input** *policy-map-name* command.

Rate-limiting (policing) of input traffic from the control plane is performed in silent mode. In silent mode, a router that is running Cisco IOS XE software operates without receiving any system messages. If a packet that is entering the control plane is discarded for input policing, you do not receive an error message.

How to Use Control Plane Policing

Defining Control Plane Services

Perform this task to define control plane services, such as packet rate control and silent packet discard for the RP.

Before you begin

Before you enter control-plane configuration mode to attach an existing QoS policy to the control plane, you must first create the policy using MQC to define a class map and policy map for control plane traffic.

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control plane interface.
- Input policing does not provide any performance benefits. It simply controls the information that is entering the device.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **control-plane**

Example:

```
Device(config)# control-plane
```

Enters control-plane configuration mode (which is a prerequisite for defining control plane services).

Step 4 **service-policy** [**input** |**output**] *policy-map-name*

Example:

```
Device(config-cp)# service-policy input control-plane-policy
```

Attaches a QoS service policy to the control plane.

- **input**—Applies the specified service policy to packets received on the control plane.

- *policy-map-name*—Name of a service policy map (created using the **policy-map** command) to be attached.

Step 5 **end**

Example:

```
Device(config-cp)# end
```

(Optional) Returns to privileged EXEC mode.

Configuration Examples for Control Plane Policing

Example: Configuring Control Plane Policing on Input Telnet Traffic

The following example shows how to apply a QoS policy for aggregate control plane services to Telnet traffic that is received on the control plane. Trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 forward Telnet packets to the control plane but are still policed for a maximum rate.

All remaining Telnet packets are dropped by the control-plane.

```
! Define trusted host traffic.
DEVICE(config)#ip access-list extended telnet-trust
DEVICE(config-ext-nacl)#10 permit tcp host 10.1.1.1 any eq telnet
DEVICE(config-ext-nacl)#20 permit tcp host 10.1.1.2 any eq telnet
DEVICE(config-ext-nacl)#exit

! Define all other Telnet traffic.
DEVICE(config)#ip access-list extended telnet-drop
DEVICE(config-ext-nacl)#10 permit tcp any any eq telnet
DEVICE(config-ext-nacl)#exit

! Define class map for trusted hosts
DEVICE(config)#class-map match-all copp-trust
DEVICE(config-cmap)#match access-group name telnet-trust
DEVICE(config-cmap)#exit

! Define class map for un-trusted hosts
DEVICE(config)#class-map match-all copp-drop
DEVICE(config-cmap)#match access-group name telnet-drop
DEVICE(config-cmap)#exit

! Define the policy-map for both type of hosts
DEVICE(config)#policy-map control-plane-in
DEVICE(config-pmap)#class copp-trust
DEVICE(config-pmap-c)#police 1000000 conform-action transmit  exceed-action drop
DEVICE(config-pmap-c-police)#class copp-drop
DEVICE(config-pmap-c-police)#exit
DEVICE(config-pmap-c)#police 1000000 conform-action drop  exceed-action drop
DEVICE(config-pmap-c-police)#exit
DEVICE(config-pmap-c)#exit
DEVICE(config-pmap)#exit

! Define aggregate control plane service for the active route processor.
DEVICE((config)#control-plane
DEVICE(config-cp)#service-policy input control-plane-in
DEVICE(config-cp)#end


! Rate-limit all other Telnet traffic.
Device(config)# access-list 140 permit tcp any any eq telnet
```

```
! Define class-map "telnet-class."
Device(config)# class-map telnet-class
Device(config-cmap)# match access-group 140
Device(config-cmap)# exit
Device(config)# policy-map control-plane-in
Device(config-pmap)# class telnet-class
Device(config-pmap-c)# police 80000 conform transmit exceed drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit

! Define aggregate control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy input control-plane-in
Device(config-cp)# end
```

Verification Examples for CoPP

The following example shows how to verify control plane policing on a policy map.

```
Router# show policy-map control-plane
           Control Plane
         Service-policy input: control-plane-in
         Class-map: telnet-class (match-all)
           10521 packets, 673344 bytes
           5 minute offered rate 18000 bps, drop rate 15000 bps
           Match: access-group 102
           police:  cir 64000 bps, bc 8000 bytes
           conformed 1430 packets, 91520 bytes; actions:
           transmit
           exceeded 9091 packets, 581824 bytes; actions:
           drop
          conformed 2000 bps, exceeded 15000 bps
     Class-map: class-default (match-any)
           0 packets, 0 bytes
           5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: any
```

The following command is used to verify the TCAM usage on the router.

```
Router# show platform hardware pp active feature qos resource-summary 0
RSP3 QoS Resource Summary

Type Total Used Free
----------------------------------------------------------------------------
QoS TCAM 2048 2 2046
VOQs 49152 808 48344
QoS Policers 32768 2 32766
QoS Policer Profiles 1023 1 1022
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 0 32768
```

QoS Support on Port Channel LACP Active Active

Link Aggregation Control Protocol (LACP) supports the automatic creation of ether channels by exchanging LACP packets between LAN ports. Cisco IOS XE Everest 16.6.1 release introduces the support of QoS on port channel LACP active active mode. A maximum of eight member links form a port channel and thus the traffic is transported through the port channel. This feature is supported on Cisco RSP3 Module.

Benefits of QoS Support on Port Channel LACP Active Active

- This feature facilitates increased bandwidth.
- The feature supports load balancing.
- This features allows support on QoS on Port Channel with one or more active member links.

Restrictions for QoS Support on Port Channel Active Active

- Policy-map on member links is not supported.
- 100G ports and 40G ports cannot be a part of the port channel.
- Total number of port channel bandwidth supported on a given ASIC should not exceed 80G.
- This feature is not supported on multicast traffic.
- Only 3k service instance (EFP) scale is supported on port channel active active.
- Ensure that 2-3 seconds of delay is maintained before and after unconfiguring and re-configuring the port channel with the **platform qos-port-channel_multiple_active** command.

Note This delay increases when you have scaled EVC configurations on the port channel.

Configuring QoS Support on Port Channel Active Active

Enabling Port Channel Active/Active

Use the following commands to enable port channel active active:

```
enable
configure terminal
sdm prefer enable_portchannel_qos_multiple_active
end
```

Note The device restarts after enabling the **sdm prefer enable_portchannel_qos_multiple_active** command. After a successful reboot, verify the configuration using the command **show sdm prefer current**

Disabling Port Channel Active/Active

Use the following commands to disable port channel active active:

```
enable
configure terminal
sdm prefer disable_portchannel_qos_multiple_active
end
```

Configuring Active Active Port Channel per bundle

Use the following commands to configure active active port channel per bundle:

```
enable
configure terminal
platform qos-port-channel_multiple_active 10
end
```

Creating Port Channel Interface

Use the following commands to configure the port channel interface:

```
enable
configure terminal
interface port-channel 10
no shutdown
end
```

Attaching member link to port channel

Use the following commands to attach a member link to the port channel:

```
enable
configure terminal
interface Te0/4/0
channel-group 10 mode active
end
```

Configuring QoS Class Map and Policy Map

Use the following commands to configure QoS class map and policy map:

```
enable
configure terminal
class-map match-any qos1
match qos-group 1
class-map match-any qos2
match qos-group 2
policy-map policymapqos
class qos1
shape average 10000 k
class qos2
shape average 20000 k
end
```

Attaching Configured Policy Map (policymapqos) on Port Channel Interface on Egress Direction

Use the following commands to attach the configured policy map (policymapqos) on the port channel interface on egress direction:

```
enable
configure terminal
interface port-channel 10
service-policy output policymapqos
end
```

Verification of QoS Support on Port Channel LACP Active Active

Use the commands below to verify the port channel summary details:

```
Device#show etherchannel summary
 Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


 Number of channel-groups in use: 1
 Number of aggregators:           1

 Group  Port-channel  Protocol    Ports
 ------+-------------+-----------+-----------------------------------------------
 10      Po10(RU)         LACP     Te0/4/0(bndl)
```

Use the commands below to verify the attached policy map on the port channel interface:

```
Device#show policy-map interface brief
Service-policy input: ingress
TenGigabitEthernet0/4/0
Service-policy output: policymapqos
Port-channel10

      Device#show policy-map interface po10
  Port-channel10

     Service-policy output: policymapqos

     Class-map: qos1 (match-any)
       1027951 packets, 1564541422 bytes
       30 second offered rate 50063000 bps, drop rate 40020000 bps
       Match: qos-group 1
       Queueing
       queue limit 819200 us/ 1024000 bytes
       (queue depth/total drops/no-buffer drops) 0/821727/0
       (pkts output/bytes output) 206224/313872928
       shape (average) cir 10000000, bc 40000, be 40000
       target shape rate 10000000

     Class-map: qos2 (match-any)
       852818 packets, 1297988996 bytes
       30 second offered rate 41534000 bps, drop rate 21447000 bps
       Match: qos-group 2
       Queueing
       queue limit 409600 us/ 1024000 bytes
       (queue depth/total drops/no-buffer drops) 0/440370/0
       (pkts output/bytes output) 412448/627745856
       shape (average) cir 20000000, bc 80000, be 80000
       target shape rate 20000000

     Class-map: class-default (match-any)
       1565 packets, 118342 bytes
       30 second offered rate 3000 bps, drop rate 0000 bps
       Match: any

       queue limit 102 us/ 1024000 bytes
       (queue depth/total drops/no-buffer drops) 0/0/0
       (pkts output/bytes output) 1565/118342
```

Use the commands below to verify the configuration after enabling port channel active/active mode:

```
#show sdm prefer current
The current sdm template is "default"
The current portchannel template is "enable_portchannel_qos_multiple_active"
```

Match Inner DSCP on RSP3 Module

Starting with Cisco IOS XE Release 16.6.1, the match_inner_dscp template is introduced. This template allows DSCP policy map configuration on the RSP3 module for MPLS and tunnel terminated traffic.

Restrictions for Match Inner DSCP on RSP3 Module

- The IPv4 DSCP policy map configuration is not preserved in case of protection scenarios, where either primary or backup path is plane IP path and backup or primary is MPLS label path.
- Match on Inner DSCP for IPv6 is not supported.
- Only 1024 entries IPv4 TCAM entries are available. Hence, optimized usage of classes is recommended for configuration when policy map is applied on port channel or port or EFP.
- To support match on Inner DSCP for IPv4 when packets have MPLS forwarding type, three TCAM entries are added whenever there is a class map with match DSCP is configured.

  One match is for normal DSCP scenario, one entry for Inner DSCP when outer header is MPLS header and other entry is when there is tunnel termination.

  In Split Horizon template, each match DSCP class consumes 3 TCAM entries. For non-Split Horizon template, TCAM entries are one. For Class default, number of entries consumed is one. For TEFP, six entries are required for each match DSCP Class Map and two for class default.

Note Some of the IPv4 qualifiers are not supported when Split Horizon template is configured as there are limitation of Copy Engines in IPv4 Resource database. Whenever Split Horizon template is enabled, four new qualifiers are added in IPV4 QoS Field Group.

Configuring Match Inner DSCP on RSP3 Module

```
Class-map match-any dscp
Match dscp af13
exit
policy-map matchdscp
Class dscp
Police cir 1000000end
```

Verifying Match Inner DSCP on RSP3 Module

```
Router# show platform hardware pp active feature qos resource-summary 0
PE1#res
RSP3 QoS Resource Summary

Type                                      Total       Used        Free
----------------------------------------------------------------------------
QoS TCAM                                  1024         0          1024
VOQs                                      49152       408         48744
QoS Policers                              32768        0          32768
QoS Policer Profiles                      1023         0          1023
Ingress CoS Marking Profiles              16           1          15
Egress CoS Marking Profiles               16           1          15
Ingress Exp & QoS-Group Marking Profiles  64           3          61
Ingress QOS LPM Entries                   32768        0          32768
```

Limitations for VLAN Translation with SDM Template for RSP3

Table 32: Feature History

Feature Name	Release Information	Feature Description
VLAN Translation for RSP3	Cisco IOS XE Bengaluru 17.4.1	VLAN translation provides flexibility in managing VLANs and Metro Ethernet-related services. You can configure 1:1 and 2:1 VLAN translations using the **sdm prefer enable_vlan_translation** command on the Cisco RSP3 module.

- On a dual RSP setup for the Cisco RSP3 module, enabling or disabling VLAN Translation template reloads the standby RP. Once standby RSP boots up, the system reaches SSO (Hot Standby State). A manual SSO (RP switchover) should to be performed before configuring any VLAN translation.

Note On a single RSP setup for the Cisco RSP3 module, enabling or disabling VLAN Translation template will save the configuration and reload the system.

Configuring VLAN Translation for RSP3

Below is sample configuration to VLAN Translation on Cisco RSP3 module.

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.

Step 3	sdm prefer enable_vlan_translation
	Example:
	`sdm prefer enable_vlan_translation`
	
	`Router(config)#sdm prefer`
	`enable_vlan_translation`
	`Standby is reloaded, it will come up with`
	` init required for new template`
	`once standby comes up`
	`Please trigger SSO`
	`Changes to VLAN Translation template`
	`stored`
		Enables VLAN Translation on the Cisco RSP3 module.

Step 4	sdm prefer disable_vlan_translation **Example:** `sdm prefer disable_vlan_translation`	Disables VLAN Translation on the Cisco RSP3 module.

	Command or Action	Purpose

	`Router(config)#sdm prefer`
	`disable_vlan_translation`
	`Standby is reloaded, it will come up with`
	` init required for new template`
	`once standby comes up`
	`Please trigger SSO`
	`Changes to VLAN Translation template`
	`stored`	

DHCP Snooping

Table 33: Feature History

Feature Name	Release Information	Feature Description
Enable DHCP Snooping Option 82 for RSP3	Cisco IOS XE Dublin 17.10.1	You can enable DHCP snooping option-82 on the Cisco RSP3 module using the **sdm prefer enable_dhcp_snoop** command. This feature provides additional security information to the relay agent that the information is from the trusted port.

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. It validates DHCP messages received from untrusted sources and filters out invalid messages. Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses. Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

DHCP Option-82

Option-82 in DHCP is an additional security mechanism over DHCP snooping. The DHCP Relay Agent Information option (Option 82) allows the DHCP Relay Agent to insert additional information into a request that is being forwarded to a DHCP server. The interface that receives “Option 82” must be a “trusted” port. If not, the packet is dropped.

The RSP3 platform supports DHCP or DHCP Snooping (option 82) feature currently using ASIC-supported system level DHCP-traps mechanism. The available DHCP-traps works at router level and traps the DHCP frames that ingress on any of the interfaces of router to CPU once enabled. Not all the DHCP frames on all types of service instances or interfaces need to be trapped to CPU. The DHCP frames that ingress on cross connect like service instances could be forwarded in data plane and does not need to be trapped to CPU always, which could avoid congestion of CPU queues further does not block the services.

Limitations for DHCP Snooping Option-82

- The Layer 2 ACL scale reduced from 512 to 256.
- The Layer 2 ACLs cannot use SRC MAC-based qualifiers.
- CFM over VPLS is not supported.

- The feature is supported only on the **enable_dhcp_snoop** template.
- The enable_dhcp_snoop and enable_l2pt_fwd_all templates are mutually exclusive.
- Maximum supported BD with DHCP snooping enabled is 10.
- A maximum of 20 EFPs can be associated to a BD which is configured with DHCP snooping. For example, single BD can be mapped to 20 EFPs or 2 to 3 BDs can also be mapped to 20 EFPs.
- This feature is supported only in normal EFP. TEFP and port-channel features are not supported for this template.
- The echo-BFD feature is not supported in the **enable_dhcp_snoop** template.
- DHCP snooping over VPLS is not supported in any of the templates.
- Layer 2 ACL is not supported on the DHCP-snooping enabled EFP.
- The scale of Layer 3 ACL is reduced from 512 to 256.

Enabling DHCP Snooping Template

To configure DHCP snooping on a service instance, use the following commands:

```
router>enable
router#configure terminal
router(config)#sdm prefer enable_dhcp_snoop
router(config-if)#end
```

After the SDM template update, the device reloads automatically and you need to enter *yes* to save the configuration.