CONTENTS

Full Cisco Trademarks with Software License  

CHAPTER 1

Using Cisco IOS XE Software 1

Understanding Command Modes 1
Understanding Diagnostic Mode 3
Accessing the CLI Using a Console 4

Accessing the CLI Using a Directly-Connected Console 4
Connecting to the Console Port 4
Using the Console Interface 5

Accessing the CLI from a Remote Console Using Telnet 6

Preparing to Connect to the Router Console Using Telnet 6
Using Telnet to Access a Console Interface 6
Accessing the CLI from a Remote Console Using a Modem 8

Using the Auxiliary Port 8
Using Keyboard Shortcuts 8
Using the History Buffer to Recall Commands 9
Getting Help 9

Finding Command Options Example 10

Using the no and default Forms of Commands 13
Saving Configuration Changes 13
Managing Configuration Files 13
Filtering Output from the show and more Commands 15
Powering Off the Router 15

Finding Support Information for Platforms and Cisco Software Images 15

Using Cisco Feature Navigator 16
Using Software Advisor 16
Using Software Release Notes 16

CHAPTER 2

Console Port Telnet and SSH Handling 17
  Important Notes and Restrictions 17
  Console Port Overview 17
  Connecting Console Cables 18
  Installing USB Device Drivers 18
  Console Port Handling Overview 18
  Telnet and SSH Overview 18
  Persistent Telnet and Persistent SSH Overview 18
  Configuring a Console Port Transport Map 19
    Examples 21
  Configuring Persistent Telnet 21
    Examples 23
  Configuring Persistent SSH 23
    Examples 26
  Viewing Console Port, SSH, and Telnet Handling Configurations 27

CHAPTER 3

Configuring Clocking and Timing 31
  Clocking and Timing Restrictions 31
    Restrictions on RSP3 Module 33
  Clocking and Timing Overview 33
    Understanding PTP 34
      Telecom Profiles 35
      PTP Redundancy 35
        PTP Redundancy Using Hop-By-Hop Topology Design 35
      Best Master Clock Algorithm 40
      Hybrid Clocking 41
      Transparent Clocking 41
      Time of Day (TOD) 42
  Timing Port Specifications 42
    BITS Framing Support 42
  Understanding Synchronous Ethernet ESMC and SSM 43
    Clock Selection Modes 43
Contents

CHAPTER 5 Configuring Ethernet Interfaces 93

Configuring Ethernet Interfaces 93
Limitations and Restrictions 93
Configuring an Interface 94
Specifying the Interface Address on an Interface Module 96
Configuring Hot Standby Router Protocol 97
Verifying HSRP 98
Modifying the Interface MTU Size 98
Interface MTU Configuration Guidelines 99
Configuring Interface MTU 99
Verifying the MTU Size 99
Configuring the Encapsulation Type 100
Configuring Autonegotiation on an Interface 100
Enabling Autonegotiation 100
Disabling Autonegotiation 100
Configuring Carrier Ethernet Features 101
Saving the Configuration 101
Shutting Down and Restarting an Interface 101
Verifying the Interface Configuration 102
Verifying Per-Port Interface Status 102
Verifying Interface Module Status 103
Configuring LAN/WAN-PHY Controllers 104
Restrictions for LAN/WAN-PHY Mode 104
Configuring LAN-PHY Mode 105
Example: Framing and Encapsulation Configuration 131
Example: CRC Configuration 131
Example: Facility Data Link Configuration 132
Example: Invert Data on the T1/E1 Interface 132

CHAPTER 7
Configuring Serial Interfaces 133
Information About Serial Interface Module 133
Restrictions 134
How to Configure Serial Interface 135
Required Configuration Tasks 135
Configuring the Controller 135
Optional Configurations 136
Configuring Layer 1 on Sync and Async Interface Server 136
Configuring Layer 1 on Sync and Async Interface Client 138
Configuring a Channel Group 140
Configuring Encapsulation 141
Configuring Transparent Pseudowire (PW) Cross-Connect 142
Configuring Invert Clock Signal 143
Configuring NRZI Formats 143
Saving the Configuration 144
Verifying the Serial Interface Configuration 144
Configuration Examples 146
Example: Encapsulation Configuration 146

CHAPTER 8
Dying Gasp Support for Loss of Power Supply via SNMP, Syslog and Ethernet OAM 147
Prerequisites for Dying Gasp Support 147
Restrictions for Dying Gasp Support 147
Configuration Examples for Dying Gasp Support 148
Configuring SNMP Community Strings on a Router 148
Configuring SNMP-Server Host Details on the Router Console 148
Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations 148
Environmental Settings on the Network Management Server 148
Message Displayed on the Peer Router on Receiving Dying Gasp Notification 150
Displaying SNMP Configuration for Receiving Dying Gasp Notification 150
Chapter 13: Operating Modes

Full Subscription Mode

Over Subscription Mode

SADT Mode

Bandwidth Mode

Slot Support on Operating Modes

IOS Port Numbering

Supported Features on the Interface Module

Benefits

Restrictions

Configuring Interface Module

Example: Configuring Full Subscription Modes

Example: Configuring Over Subscription Modes

Verifying Configuration

Verifying High Priority and Low Priority Counters Configuration

Configuring Bandwidth Mode

Verifying Bandwidth Mode Configuration
CHAPTER 14

Card Protection for 48-Port T1/E1 CEM and 48-Port T3/E3 CEM Interface Modules 245

Y Cable 246
Card Protection Switchover 246
Alarm Based Switchover 247
Restrictions 247
Supported Features on Interface Module 247
Configuring Maintenance Commands 248
Priority Table 248
Configuring T3/E3 Card Protection 248
Configuring Revertive Mode 250
Verifying T3/E3 Card Protection Configuration 250
Configuring T1/E1 Card Protection 251
Configuring Revertive Mode 251
Verification of T1/E1 Card Protection Configuration 252

Associated Commands 252
Additional References 253

CHAPTER 15

Configuring 1G Traffic on 8-port 10 Gigabit Ethernet Interface Module 255

Restrictions for 1G Mode on 8X10 GE Interface Module 255
Configuring 1G Mode 256
Verifying 1G Mode Configuration 256
Configuring 10G Mode from 1G Mode 257
Verifying 10G Mode Configuration 257

Associated Commands 258

Overview of Over Subscription and Partial Port Modes on the 8-port 10 Gigabit Ethernet Interface Module 259

Over Subscription Mode 259
Partial Port Mode 260

Prerequisites for Over Subscription Mode on the 8-port 10 Gigabit Ethernet Interface Module 260
Restrictions for Over Subscription Mode 8-port 10 Gigabit Ethernet Interface Module 260
CHAPTER 16

Configuring the SDM Template 265

Prerequisites for the SDM Template 265
Restrictions for the SDM Template 265
Information About the SDM Template 267
Selecting the SDM Template 278
Verifying the SDM Template 280

SDM Template Supported Features on RSP3 Module 280

VPLS Statistics 281

Split Horizon Enhancements on the RSP3 Module 282

Prerequisites for Split-Horizon Groups on the RSP3 Module 282
Restrictions for Split-Horizon Groups on the RSP3 Module 282
Split-Horizon Supported Scale 283
Configuring Split-Horizon Group on the RSP3 Module 283

8K EFP (4 Queue Model) 283

Information About 8000 (8K) EFP 283
Prerequisites for 8000 (8K) EFP 284
Restrictions for 8000 (8K) EFP 284
Configuring 8K Model 284

16K EFP Support on Port Channel 287

Restrictions for 16K EFP on Port Channel 287
Configuring 16K EFP on Port Channel 288
Verifying 16k EFP on Port Channel 288

Control Plane Policing 289

Restrictions for Control Plane Policing 289
Restrictions for CoPP on the RSP3 289
Supported Protocols 290
Input Rate-Limiting and Silent Mode Operation 292
How to Use Control Plane Policing 292
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 2 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>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Log in.</td>
<td>Router&gt;</td>
<td>Use the logout command.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>From user EXEC mode, use the enable EXEC command.</td>
<td>Router#</td>
<td>To return to user EXEC mode, use the disable command.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>From privileged EXEC mode, use the configure terminal privileged EXEC command.</td>
<td>Router(config)#</td>
<td>To return to privileged EXEC mode from global configuration mode, use the exit or end command.</td>
</tr>
<tr>
<td>Interface configuration</td>
<td>From global configuration mode, specify an interface using an interface command.</td>
<td>Router(config-if)#</td>
<td>To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.</td>
</tr>
</tbody>
</table>
| 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 1 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. |
### 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.

------------

#### 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.
• 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.

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).

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:

**SUMMARY STEPS**

1. Configure your terminal emulation software with the following settings:
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”).

**DETAILED STEPS**

**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:

SUMMARY STEPS

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.

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

   Example:
   
   Router>

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

   Example:
   
   Router> enable

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

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

   Example:
   
   Router#

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

7. To exit the console session, enter the `quit` command as shown in the following example:

   Example:
   
   Router> quit

DETAILED STEPS

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 `quit` command as shown in the following example:

Example:

```
Router# quit
```

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.

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:

**SUMMARY STEPS**

1. From your terminal or PC, enter one of the following commands:
2. At the password prompt, enter your login password. The following example shows entry of the password called “mypass”:
3. From user EXEC mode, enter the `enable` command as shown in the following example:
4. At the password prompt, enter your system password. The following example shows entry of the password called “enablepass”:
5. When the enable password is accepted, the privileged EXEC mode prompt appears:
6. You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.
7. To exit the Telnet session, use the `exit` or `logout` command as shown in the following example:
DETAILED STEPS

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:**
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 2: Keyboard Shortcuts, on page 8 lists the keyboard shortcuts for entering and editing commands.

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-B or the Left Arrow key</td>
<td>Move the cursor back one character</td>
</tr>
<tr>
<td>Ctrl-F or the Right Arrow key</td>
<td>Move the cursor forward one character</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Move the cursor to the beginning of the command line</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Move the cursor to the end of the command line</td>
</tr>
<tr>
<td>Esc B</td>
<td>Move the cursor back one word</td>
</tr>
<tr>
<td>Esc F</td>
<td>Move the cursor forward one word</td>
</tr>
</tbody>
</table>

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 3: History Substitution Commands, on page 9 lists the history substitution commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P or the Up Arrow key²</td>
<td>Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl-N or the Down Arrow key¹</td>
<td>Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key.</td>
</tr>
<tr>
<td>Router# show history</td>
<td>While in EXEC mode, list the last several commands you have just entered.</td>
</tr>
</tbody>
</table>

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 4: Help Commands and Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Provides a brief description of the help system in any command mode.</td>
</tr>
<tr>
<td>abbreviated-command-entry ?</td>
<td>Provides a list of commands that begin with a particular character string. (No space between command and question mark.)</td>
</tr>
<tr>
<td>abbreviated-command-entry &lt;Tab&gt;</td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td>command ?</td>
<td>Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)</td>
</tr>
</tbody>
</table>
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 5: Finding Command Options, on page 10 shows examples of how you can use the question mark (?) to assist you in entering commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
</table>
| 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?`  
`<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)#`. |
Enter `?` 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
</table>
| Router(config-if)# ? | **Interface configuration commands:**
| | .
| | .
| | ip)
| | Interface Internet Protocol config commands
| | keepalive Enable keepalive
| | lan-name LAN Name command
| | lloc Interface LLC2 Interface Subcommands
| | load-interval Specify interval for load calculation for an interface
| | locaddr-priority Assign a priority group
| | logging Configure logging for interface
| | loadback 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)# |
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
</table>
| 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|

**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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
</table>
| Router(config-if)# **ip address ?**
  A.B.C.D IP address
  negotiated IP Address negotiated over PPP|

**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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
</table>
| Router(config-if)# **ip address 172.16.0.1 ?**
  A.B.C.D IP subnet mask|

**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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
</table>
| Router(config-if)# **ip address 172.16.0.1 255.255.255.0 ?**
  secondary Make this IP address a secondary address
  <cr>|

**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.
Using Cisco IOS XE Software

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**

```bash
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 (119948064 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**

```bash
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.bin
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**

```bash
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]
```

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.
This chapter covers the following topics:

- Important Notes and Restrictions, on page 17
- Console Port Overview, on page 17
- Connecting Console Cables, on page 18
- Installing USB Device Drivers, on page 18
- Console Port Handling Overview, on page 18
- Telnet and SSH Overview, on page 18
- Persistent Telnet and Persistent SSH Overview, on page 18
- Configuring a Console Port Transport Map, on page 19
- Configuring Persistent Telnet, on page 21
- Configuring Persistent SSH, on page 23
- Viewing Console Port, SSH, and Telnet Handling Configurations, on page 27

### 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 is 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 located at http://www.cisco.com/en/US/docs/ios/12_2/termserv/command/reference/trflosho.html#wp1029818.

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 21 and the Configuring Persistent SSH, on page 23.

Configuring a Console Port Transport Map

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

**SUMMARY STEPS**

1. enable
2. configure terminal
3. transport-map type console transport-map-name
4. connection wait [allow interruptible | none]
5. banner [diagnostic | wait] banner-message
6. exit
7. transport type console console-line-number input transport-map-name

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>transport-map type console transport-map-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# transport-map type console consolehandler</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Creates and names a transport map for handling console connections, and enter transport map configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies how a console connection will be handled using this transport map:</td>
<td></td>
</tr>
<tr>
<td>connection wait [allow interruptible</td>
<td>• 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 line to become available. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td>none]</td>
<td>• none—The console connection immediately enters diagnostic mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-tmap)# connection wait none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(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.</td>
<td></td>
</tr>
<tr>
<td>banner [diagnostic</td>
<td>• diagnostic—Creates a banner message seen by users directed into diagnostic mode as a result of the console transport map configuration.</td>
<td></td>
</tr>
<tr>
<td>wait] banner-message</td>
<td>• wait—Creates a banner message seen by users waiting for the IOS vty to become available.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>• banner-message—The banner message, which begins and ends with the same delimiting character.</td>
<td></td>
</tr>
<tr>
<td>Router(config-tmap)# banner diagnostic X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter TEXT message. End with the character 'X'.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--Welcome to Diagnostic Mode--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-tmap)#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits transport map configuration mode to re-enter global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-tmap)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Applies the settings defined in the transport map to the console interface.</td>
<td></td>
</tr>
<tr>
<td>transport type console console-line-number input transport-map-name</td>
<td>The transport-map-name for this command must match the transport-map-name defined in the transport-map type console comm and.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config)# transport type console 0 input consolehandler</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

SUMMARY STEPS

1. enable
2. configure terminal
3. transport-map type persistent telnet transport-map-name
4. connection wait [allow {interruptible}] [none {disconnect}]
5. banner [diagnostic | wait] banner-message
6. transport interface type num
7. exit
8. transport type persistent telnet input transport-map-name

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Persistent Telnet

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# configure terminal</td>
<td>Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.</td>
</tr>
</tbody>
</table>

### Step 3

**transport-map type persistent telnet transport-map-name**

**Example:**

```bash
Router(config)# transport-map type persistent telnet telnethandler
```

### Step 4

**connection wait [allow {interruptible} | none {disconnect}]**

**Example:**

```bash
Router(config-tmap)# connection wait none
```

- **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 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:**

```bash
Router(config-tmap)# banner diagnostic X
```

- **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.

(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.
### Purpose

Command or Action                                              Purpose

<table>
<thead>
<tr>
<th>Step 6</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>transport interface type <em>num</em></td>
<td>Applies the transport map settings to the Management Ethernet</td>
</tr>
<tr>
<td>Example:</td>
<td>interface (interface gigabitethernet 0).</td>
</tr>
<tr>
<td>Router(config-tmap)# transport interface</td>
<td>Persistent Telnet can only be applied to the Management</td>
</tr>
<tr>
<td>gigabitethernet 0</td>
<td>Ethernet interface on the chassis. This step must be taken</td>
</tr>
<tr>
<td></td>
<td>before applying the transport map to the Management</td>
</tr>
<tr>
<td></td>
<td>Ethernet interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Exits transport map configuration mode to re-enter global</td>
</tr>
<tr>
<td>exit</td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-tmap)# exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>Applies the settings defined in the transport map to the</td>
</tr>
<tr>
<td>transport type persistent telnet input <em>transport-map-name</em></td>
<td>Management Ethernet interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>The <em>transport-map-name</em> for this command must match the</td>
</tr>
<tr>
<td>Router(config)# transport type persistent telnet</td>
<td>transport-map-name defined in the transport-map type</td>
</tr>
<tr>
<td>input telnethandler</td>
<td>persistent telnet command.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

#### 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.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `transport-map type persistent ssh transport-map-name`
4. `connection wait [allow {interruptible}] | none {disconnect}]`
5. `rsa keypair-name rsa-keypair-name`
6. `authentication-retries number-of-retries`
7. `banner [diagnostic | wait] banner-message`
8. `time-out timeout-interval`
9. `transport interface type num`
10. `exit`
11. `transport type persistent ssh input transport-map-name`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>transport-map type persistent ssh transport-map-name</code></td>
<td>Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# <code>transport-map type persistent ssh sshhandler</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `connection wait [allow {interruptible}]</td>
<td>none {disconnect}]`</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-tmap)# <code>connection wait allow interruptible</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. 

- **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.
- **none**—The SSH connection immediately enters diagnostic mode.
### Configuring Persistent SSH

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>none disconnect</strong>—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.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Names the RSA keypair to be used for persistent SSH connections.</td>
</tr>
<tr>
<td><strong>rsa keypair-name</strong></td>
<td>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 <code>ip ssh rsa keypair-name</code> command, do not apply to persistent SSH connections.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>No <code>rsa-keypair-name</code> is defined by default.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specifies the number of authentication retries before dropping the connection. The default <code>number-of-retries</code> is 3.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>authentication-retries</strong></td>
<td>• <strong>diagnostic</strong>—Creates a banner message seen by users directed into diagnostic mode as a result of the persistent SSH configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• <strong>wait</strong>—Creates a banner message seen by users waiting for the vty line to become active.</td>
</tr>
<tr>
<td></td>
<td>• <strong>banner-message</strong>—The banner message, which begins and ends with the same delimiting character.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specifies the SSH time-out interval in seconds. The default <code>timeout-interval</code> is 120 seconds.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>transport interface type num</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Router(config-tmap)# rsa keypair-name sshkeys</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Router(config-tmap)# transport interface gigabitethernet 0</code></td>
<td>Exits transport map configuration mode to re-enter global configuration mode.</td>
</tr>
</tbody>
</table>

**Step 10**

**Example:**

`Router(config-tmap)# exit`

Applies the settings defined in the transport map to the Management Ethernet interface.

**Step 11**

**transport type persistent ssh input transport-map-name**

**Example:**

`Router(config)# transport type persistent ssh input sshhandler`

The `transport-map-name` for this command must match the `transport-map-name` defined 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
Welcome to Diagnostic Mode
Waiting for IOS Process
Method : ssh
Rule : wait

Welcome to Diagnostic Mode
Waiting for IOS
Method : console
Rule : wait with interrupt

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config-tmap)# 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
Welcome to Diagnostic Mode
Waiting for IOS process
Method : ssh
Rule : wait with interrupt
Welcome to Diag Mode
Waiting for IOS
Method : console
Rule : wait with interrupt
Welcome to Diag Mode
Waiting for IOS
Method : console
Rule : wait with interrupt
CHAPTER 3

Configuring Clocking and Timing

This chapter explains how to configure timing ports on the Route Switch Processor (RSP) modules and includes the following sections:

- Clocking and Timing Restrictions, on page 31
- Clocking and Timing Overview, on page 33
- Configuring Clocking and Timing, on page 44
- Verifying the Configuration, on page 78
- Troubleshooting, on page 79
- Configuration Examples, on page 80

Clocking and Timing Restrictions

The following clocking and timing restrictions apply to the chassis:

- Interfaces carrying PTP traffic must be under the same VPN Routing and Forwarding (VRF). Misconfiguration will cause PTP packet loss.
  Use the 10 Gigabit Links to configure VRF on two Cisco RSP3 Routers.
- You can configure only a single clocking input source within each group of eight ports (0–7 and 8–15) on the T1/E1 interface module using the `network-clock input-source` command.
- Multicast timing is not supported.
- Out-of-band clocking and the `recovered-clock` command are not supported.
- Precision Time Protocol (PTP) is supported only on loopback interfaces.
- Synchronous Ethernet clock sources are not supported with PTP. Conversely, PTP clock sources are not supported with synchronous Ethernet except when configured as hybrid clock. However, you can use hybrid clocking to allow the chassis to obtain frequency using Synchronous Ethernet, and phase using PTP.
- Time of Day (ToD) and 1 Pulse per Second (1PPS) input is not supported when the chassis is in boundary clock mode.
- Multiple ToD clock sources are not supported.
- PTP redundancy is supported only on unicast negotiation mode; you can configure up to three master clocks in redundancy mode.
• In order to configure time of day input, you must configure both an input 10 Mhz and an input 1 PPS source.

• PTP over IPv6 is not supported.

• SyncE Rx and Tx is supported on uplink interfaces when using 8 x 1 GE Gigabit Ethernet SFP Interface Module.

• When PTP is configured, changing the configuration mode from LAN to WAN or WAN to LAN is not supported for following IMs:
  • 2x10G
  • 8x1G_1x10G_SFP
  • 8x1G_1x10G_CU

• PTP functionality is restricted by license type.

---

**Note**

If you install the IEEE 1588-2008 BC/MC licenseIEEE 1588-2008 BC/MC license (available by default), you must reload the chassis to use the full PTP functionality.

---

**Note**

By default, all timing licenses are already included on the Cisco NCS 4200 routers.

• End-to-end Transparent Clock is not supported for PTP over Ethernet.

• Transparent clock is not supported on the Cisco RSP3 Module.

• G.8265.1 telecom profiles are not supported with PTP over Ethernet.

• The chassis does not support a mix of IPv4 and Ethernet clock ports when acting as a transparent clock or boundary clock.

The following restrictions apply when configuring synchronous Ethernet SSM and ESMC:

• To use the `network-clock synchronization ssm option` command, ensure that the chassis configuration does not include the following:
  • Input clock source
  • Network clock quality level
  • Network clock source quality source (synchronous Ethernet interfaces)

• The `network-clock synchronization ssm option` command must be compatible with the `network-clock eec` command in the configuration.

• To use the `network-clock synchronization ssm option` command, ensure that there is not a network clocking configuration applied to synchronous Ethernet interfaces, BITS interfaces, and timing port interfaces.
• SSM and ESMC are SSO-coexistent, but not SSO-compliant. The chassis goes into hold-over mode during switchover and restarts clock selection when the switchover is complete.

• The chassis does not support ESMC messages on the S1 byte on SONET/SDH and T1/E1 interface modules.

• It is recommended that you do not configure multiple input sources with the same priority as this impacts the TSM (Switching message delay).

• You can configure a maximum of 4 clock sources on interface modules, with a maximum of 2 per interface module. This limitation applies to both synchronous Ethernet and TDM interfaces.

• When you configure the ports using the synchronous mode command on a copper interface, the port attempts to auto-negotiate with the peer-node copper port and hence the auto negotiation is incomplete as both the ports try to act as master, which in turn makes the port down. Hence, for a successful clock sync to happen, you should configure the ports using network-clock input-source / interface interface id command prior to the configuration using the synchronous mode command under the interfaces to ensure that one of the ports behaves as a master.

It is not recommended to configure the copper ports using the synchronous mode command.

Restrictions on RSP3 Module

The following clocking and timing restrictions are supported on the RSP3 Module:

• Precision Time Protocol (PTP) is supported only on the routed interfaces.

• Transparent Clock over 1 Gigabit Ethernet port performance is not good.

• PTP is supported for LAN for the following IMs. WAN is not supported.
  • 2x40
  • 1x100 GE
  • 8x10 GE

• To shift from non hybrid clock configuration to hybrid clock configuration, you must first unconfigure PTP, unconfigure netsync, reconfigure netsync and configure hybrid PTP.

Clocking and Timing Overview

The chassis have the following timing ports:

• 1 PPS Input/Output
• 10 Mhz Input/Output
• ToD
• Building Integrated Timing Supply (BITS)

You can use the timing ports on the chassis to perform the following tasks:

• Provide or receive 1 PPS messages
• Provide or receive time of day (ToD) messages
• Provide output clocking at 10 Mhz, 2.048 Mhz, and 1.544 Mhz
• Receive input clocking at 10 Mhz, 2.048 Mhz, and 1.544 Mhz

Note Timing input and output is handled by the active RSP.

Note For timing redundancy, you can use a Y cable to connect a GPS timing source to multiple RSPs. For information, see the Cisco NCS 4206 Series Hardware Installation Guide.

SyncE is supported in both LAN and WAN mode on a 10 Gigabit Ethernet interface.

The following sections describe how to configure clocking and timing features on the chassis.

Understanding PTP

The Precision Time Protocol (PTP), as defined in the IEEE 1588 standard, synchronizes with nanosecond accuracy the real-time clocks of the devices in a network. The clocks in are organized into a master-member hierarchy. PTP identifies the switch port that is connected to a device with the most precise clock. This clock is referred to as the master clock. All the other devices on the network synchronize their clocks with the master and are referred to as members. Constantly exchanged timing messages ensure continued synchronization.

PTP is particularly useful for industrial automation systems and process control networks, where motion and precision control of instrumentation and test equipment are important.

Table 6: Nodes within a PTP Network

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grandmaster (GM)</td>
<td>A network device physically attached to the primary time source. All clocks are synchronized to the grandmaster clock.</td>
</tr>
<tr>
<td>Ordinary Clock (OC)</td>
<td>An ordinary clock is a 1588 clock with a single PTP port that can operate in one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• Master mode—Distributes timing information over the network to one or more slave clocks, thus allowing the slave to synchronize its clock to the master.</td>
</tr>
<tr>
<td></td>
<td>• Slave mode—Synchronizes its clock to a master clock. You can enable the slave mode on up to two interfaces simultaneously in order to connect to two different master clocks.</td>
</tr>
<tr>
<td>Boundary Clock (BC)</td>
<td>The device participates in selecting the best master clock and can act as the master clock if no better clocks are detected.</td>
</tr>
<tr>
<td></td>
<td>Boundary clock starts its own PTP session with a number of downstream slaves. The boundary clock mitigates the number of network hops and results in packet delay variations in the packet network between the Grand Master and Slave.</td>
</tr>
<tr>
<td>Transparent Clock (TC)</td>
<td>A transparent clock is a device or a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of time calculations.</td>
</tr>
</tbody>
</table>
Telecom Profiles

Release 3.8 introduces support for telecom profiles, which allow you to configure a clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes. For information about how to configure telecom profiles, see Configuring Clocking and Timing, on page 44.

Effective Cisco IOS-XE Release 3.18, the G.8275.1 telecom profile is also supported on the Cisco NCS 4206 Series with RSP2 module. For more information, see G.8275.1 Telecom Profile.

PTP Redundancy

PTP redundancy is an implementation on different clock nodes. This helps the PTP slave clock node achieve the following:

- Interact with multiple master ports such as grand master clocks and boundary clock nodes.
- Open PTP sessions.
- Select the best master from the existing list of masters (referred to as the primary PTP master port or primary clock source).
- Switch to the next best master available in case the primary master fails, or the connectivity to the primary master fails.

Note

The Cisco NCS 4206 Series chassis supports unicast-based timing as specified in the 1588-2008 standard.

For instructions on how to configure PTP redundancy, see Configuring PTP Redundancy, on page 65.

PTP Redundancy Using Hop-By-Hop Topology Design

Real world deployments for IEEE-1588v2 for mobile backhaul requires the network elements to provide synchronization and phase accuracy over IP or MPLS networks along with redundancy.

In a ring topology, a ring of PTP boundary clock nodes are provisioned such that each boundary clock node provides synchronization to a number of PTP slaves connected to it. Each such ring includes at least two PTP masters with a PRC traceable clock.

However, with this topology the following issues may occur:

- Node asymmetry and delay variation—In a ring topology, each boundary clock uses the same master, and the PTP traffic is forwarded through intermediate boundary clock nodes. As intermediate nodes do not correct the timestamps, variable delay and asymmetry for PTP are introduced based on the other traffic passing through such nodes, thereby leading to incorrect results.
- Clock redundancy—Clock redundancy provides redundant network path when a node goes down. In a ring topology with PTP, for each unicast PTP solution, the roles of each node is configured. The PTP clock path may not be able to reverse without causing timing loops in the ring.

No On-Path Support Topology

The topology (see Figure 1: Deployment in a Ring - No On-Path Support with IPv4, on page 36) describes a ring with no on-path support. S1 to S5 are the boundary clocks that use the same master clocks. GM1 and GM2 are the grandmaster clocks. In this design, the following issues are observed:

- Timestamps are not corrected by the intermediate nodes.
- Difficult to configure the reverse clocking path for redundancy.
• Formation of timings loops.

Figure 1: Deployment in a Ring - No On-Path Support with IPv4

Table 7: PTP Ring Topology — No On-Path Support

<table>
<thead>
<tr>
<th>Clock Nodes</th>
<th>Behavior in the PTP Ring</th>
</tr>
</thead>
<tbody>
<tr>
<td>GM1</td>
<td>Grandmaster Clock</td>
</tr>
<tr>
<td>GM2</td>
<td>Grandmaster Clock</td>
</tr>
<tr>
<td>S1</td>
<td>Masters: M1 (1st), M2 (2nd)</td>
</tr>
<tr>
<td>S2</td>
<td>Masters: M1 (1st), M2 (2nd)</td>
</tr>
<tr>
<td>S3</td>
<td>Masters: M1 (1st), M2 (2nd)</td>
</tr>
<tr>
<td>S4</td>
<td>Masters: M2 (1st), M1 (2nd)</td>
</tr>
<tr>
<td>S5</td>
<td>Masters: M2 (1st), M1 (2nd)</td>
</tr>
</tbody>
</table>

A solution to the above issue is addressed by using Hop-by-Hop topology configuration.

Hop-By-Hop Topology in a PTP Ring

PTP Ring topology is designed by using Hop-By-Hop configuration of PTP boundary clocks. In this topology, each BC selects its adjacent nodes as PTP masters, instead of using the same GM as the PTP master. These PTP BC masters are traceable to the GM in the network. Timing loop are not formed between adjacent BC nodes. The hot Standby BMCA configuration is used for switching to next the best master during failure.

Prerequisites

• PTP boundary clock configuration is required on all clock nodes in the ring, except the master clock nodes (GM), which provide the clock timing to ring. In the above example (see Figure 5-1) nodes S1 ... S5 must be configured as BC.
• The master clock (GM1 and GM2 in Figure 5-1) nodes in the ring can be either an OC master or BC master.
• Instead of each BC using the same GM as a PTP master, each BC selects its adjacent nodes as PTP masters. These PTP BC-masters are traceable to the GM in the network.
• Boundary clock nodes must be configured with the single-hop keyword in the PTP configuration to ensure that a PTP node can communicate with its adjacent nodes only.

Restrictions

• Timing loops should not exist in the topology. For example, if for a node there are two paths to get the same clock back, then the topology is not valid. Consider the following topology and configuration.

The paths with double arrows (>>) are the currently active clock paths and paths with single arrow (>) are redundant clock path. This configuration results in a timing loop if the link between the BC-1 and GM fails.

• In a BC configuration, the same loopback interface should never be used for both master and slave port configuration.
• Single-hop keyword is not supported for PTP over MPLS with explicit null configuration. The Single-hop keyword is not supported when PTP packets are sent out with a MPLS tag.
On-Path Support Topology Scenario

Consider the topology as shown in Figure 5-1.

*Figure 2: PTP Ring Topology—On-Path Support*

<table>
<thead>
<tr>
<th>Clock Node</th>
<th>Behavior in the PTP Ring</th>
</tr>
</thead>
<tbody>
<tr>
<td>GM1</td>
<td>Grandmaster Clock</td>
</tr>
<tr>
<td>GM2</td>
<td>Grandmaster Clock</td>
</tr>
</tbody>
</table>
| BC1        | Masters: M1 (1st), BC2 (2nd)  
             | Slaves: BC2              |
| BC2        | Masters: BC1 (1st), BC3 (2nd)  
             | Slaves: BC1, BC3         |
| BC3        | Masters: BC2 (1st), BC4 (2nd)  
             | Slaves: BC2, BC4         |
| BC4        | Masters: BC5 (1st), BC3 (2nd)  
             | Slaves: BC3, BC5         |
| BC5        | Masters: M2 (1st), BC4 (2nd)  
             | Slaves: BC4              |

Now consider there is a failure between BC1 and BC2 (see Figure 5-3). In this case, the BC2 cannot communicate with GM1. Node BC2 receives the clock from BC3, which in turn receives the clock from GM2.
Figure 3: Deployment in a Ring—On-Path Support (Failure)

Table 9: PTP Ring Topology—On-Path Support (Failure)

<table>
<thead>
<tr>
<th>Clock Node</th>
<th>Behavior in the PTP Ring³</th>
</tr>
</thead>
<tbody>
<tr>
<td>GM1</td>
<td>Grandmaster Clock</td>
</tr>
<tr>
<td>GM2</td>
<td>Grandmaster Clock</td>
</tr>
<tr>
<td>BC1</td>
<td>Masters: M1 (1st), BC2 (2nd)</td>
</tr>
<tr>
<td></td>
<td>Slaves: BC2</td>
</tr>
<tr>
<td>BC2</td>
<td>Masters: BC1(1st), BC3 (2nd)</td>
</tr>
<tr>
<td></td>
<td>Slaves: BC1, BC3</td>
</tr>
<tr>
<td>BC3</td>
<td>Masters: BC2 (1st), BC4 (2nd)</td>
</tr>
<tr>
<td></td>
<td>Slaves: BC2, BC4</td>
</tr>
<tr>
<td>BC4</td>
<td>Masters: BC5 (1st), BC3 (2nd)</td>
</tr>
<tr>
<td></td>
<td>Slaves: BC3, BC5</td>
</tr>
</tbody>
</table>
Behavior in the PTP Ring

<table>
<thead>
<tr>
<th>Clock Node</th>
<th>Behavior in the PTP Ring</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC5</td>
<td>Masters: M2(1st), BC4 (2nd)</td>
</tr>
<tr>
<td></td>
<td>Slaves: BC4</td>
</tr>
</tbody>
</table>

3 Red indicates that GM is not traceable and there is no path to the slave.

Configuration Example

PTP Ring boundary clocks must be configured with **single-hop** keyword in PTP configuration. The PTP node can communicate with its adjacent nodes only. This is required for PTP hop-by-hop ring topology.

```plaintext
ptp clock boundary domain 0
  clock-port bcslave1 slave
    transport ipv4 unicast interface Lo0 negotiation single-hop
    clock source 1.1.1.1
  clock-source 2.2.2.2 1
  clock-port bcmaster1 master
    transport ipv4 unicast interface Lo1 negotiation single-hop
```

Note

The **single-hop** keyword is not supported for PTP over MPLS with explicit NULL configurations. The **single-hop** keyword is not supported when PTP packets are sent out with a MPLS tag.

For information on configuring PTP redundancy, see Configuring PTP Redundancy, on page 65.

Best Master Clock Algorithm

Starting Cisco IOS XE Release 3.15, Best Master Clock Algorithm (BMCA) is supported on the chassis. BMCA is used to select the master clock on each link, and ultimately, select the grandmaster clock for the entire Precision Time Protocol (PTP) domain. BCMA runs locally on each port of the ordinary and boundary clocks, and selects the best clock.

The best master clock is selected based on the following parameters:

- Priority—User-configurable value ranging from 0 to 255; lower value takes precedence
- Clock Class—Defines the traceability of time or frequency from the grandmaster clock
- Alarm Status—Defines the alarm status of a clock; lower value takes precedence

By changing the user-configurable values, network administrators can influence the way the grandmaster clock is selected.

BMCA provides the mechanism that allows all PTP clocks to dynamically select the best master clock (grandmaster) in an administration-free, fault-tolerant way, especially when the grandmaster clocks changes.

For information on configuring BMCA, see Configuring an Ordinary Clock, on page 44 and Configuring a Boundary Clock, on page 52.
Hybrid BMCA

In hybrid BMCA implementation, the phase is derived from a PTP source and frequency is derived from a physical lock source. More than one master clock is configured in this model and the best master is selected. If the physical clock does down, then PTP is impacted.

Configuration Example

**Hybrid BMCA on Ordinary Clock**

```plaintext
ptp clock ordinary domain 0 hybrid
clock-port SLAVE slave
transport ipv4 unicast interface Lo0 negotiation
clock source 133.133.133.133
clock source 144.144.144.144 1
clock source 155.155.155.155 2
Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

**Hybrid BMCA on Boundary Clock**

```plaintext
ptp clock boundary domain 0 hybrid
clock-port SLAVE slave
transport ipv4 unicast interface Lo0 negotiation
clock source 133.133.133.133
clock source 144.144.144.144 1
clock source 155.155.155.155 2
clock-port MASTER master
transport ipv4 unicast interface Lo1 negotiation
Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

Hybrid Clocking

The Cisco NCS 4206 Series Chassis support a hybrid clocking mode that uses clock frequency obtained from the synchronous Ethernet port while using the phase (ToD or 1 PPS) obtained using PTP. The combination of using physical source for frequency and PTP for time and phase improves the performance as opposed to using only PTP.

**Note**

When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same master clock.

For more information on how to configure hybrid clocking, see Configuring a Hybrid Clock, on page 56.

Transparent Clocking

A transparent clock is a network device such as a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of timing calculations. The transparent clock ports have no state because the transparent clock does not need to synchronize to the grandmaster clock.

There are two kinds of transparent clocks:

- End-to-end transparent clock—Measures the residence time of a PTP message and accumulates the times in the correction field of the PTP message or an associated follow-up message.
• Peer-to-peer transparent clock—Measures the residence time of a PTP message and computes the link delay between each port and a similarly equipped port on another node that shares the link. For a packet, this incoming link delay is added to the residence time in the correction field of the PTP message or an associated follow-up message.

Note
The Cisco NCS 4206 Series Chassis does not currently support peer-to-peer transparent clock mode.

For information on how to configure the Cisco NCS 4206 Series Chassis as a transparent clock, see Configuring a Transparent Clock, on page 55.

Time of Day (TOD)

You can use the time of day (ToD) and 1PPS ports on the Cisco NCS 4206 Series Chassis to exchange ToD clocking. In master mode, the chassis can receive time of day (ToD) clocking from an external GPS unit; the chassis requires a ToD, 1PPS, and 10MHZ connection to the GPS unit.

In slave mode, the chassis can recover ToD from a PTP session and repeat the signal on ToD and 1PPS interfaces.

For instructions on how to configure ToD on the Cisco NCS 4206 Series Chassis, see the Configuring an Ordinary Clock, on page 44.

Synchronizing the System Clock to Time of Day

You can set the chassis system time to synchronize with the time of day retrieved from an external GPS device. For information on how to configure this feature, see Synchronizing the System Time to a Time-of-Day Source, on page 69.

Timing Port Specifications

The following sections provide specifications for the timing ports on the Cisco NCS 4206 Series Chassis.

BITS Framing Support

The following table lists the supported framing modes for a BITS port.

<table>
<thead>
<tr>
<th>BITS or SSU Port Support Matrix</th>
<th>Framing Modes Supported</th>
<th>SSM or QL Support</th>
<th>Tx Port</th>
<th>Rx Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>T1 ESF</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>T1</td>
<td>T1 SF</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>E1</td>
<td>E1 CRC4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>E1</td>
<td>E1 FAS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2048 kHz</td>
<td>2048 kHz</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
The BITS port behaves similarly to the T1/E1 ports on the T1/E1 interface module; for more information about configuring T1/E1 interfaces, see the Configuring T1/E1 Interfaces document.

**Understanding Synchronous Ethernet ESMC and SSM**

Synchronous Ethernet incorporates the Synchronization Status Message (SSM) used in Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) networks. While SONET and SDH transmit the SSM in a fixed location within the frame, Ethernet Synchronization Message Channel (ESMC) transmits the SSM using a protocol: the IEEE 802.3 Organization-Specific Slow Protocol (OSSP) standard.

The ESMC carries a Quality Level (QL) value identifying the clock quality of a given synchronous Ethernet timing source. Clock quality values help a synchronous Ethernet node derive timing from the most reliable source and prevent timing loops.

When configured to use synchronous Ethernet, the chassis synchronizes to the best available clock source. If no better clock sources are available, the chassis remains synchronized to the current clock source.

The chassis supports two clock selection modes: QL-enabled and QL-disabled. Each mode uses different criteria to select the best available clock source.

For more information about Ethernet ESMC and SSM, see Configuring Synchronous Ethernet ESMC and SSM, on page 72.

---

**Note**

The chassis can only operate in one clock selection mode at a time.

**Note**

PTP clock sources are not supported with synchronous Ethernet.

**Clock Selection Modes**

The chassis supports two clock selection modes, which are described in the following sections.

**QL-Enabled Mode**

In QL-enabled mode, the chassis considers the following parameters when selecting a clock source:

- Clock quality level (QL)
- Clock availability
- Priority

**QL-Disabled Mode**

In QL-disabled mode, the chassis considers the following parameters when selecting a clock source:

- Clock availability
- Priority

**Note**

You can use override the default clock selection using the commands described in the Managing Clock Source Selection, on page 76.
Managing Clock Selection

You can manage clock selection by changing the priority of the clock sources; you can also influence clock selection by modifying the following clock properties:

- **Hold-Off Time**: If a clock source goes down, the chassis waits for a specific hold-off time before removing the clock source from the clock selection process. By default, the value of hold-off time is 300 ms.
- **Wait to Restore**: The amount of time that the chassis waits before including a newly active synchronous Ethernet clock source in clock selection. The default value is 300 seconds.
- **Force Switch**: Forces a switch to a clock source regardless of clock availability or quality.
- **Manual Switch**: Manually selects a clock source, provided the clock source has an equal or higher quality level than the current source.

For more information about how to use these features, see Managing Clock Source Selection, on page 76.

Configuring Clocking and Timing

The following sections describe how to configure clocking and timing features on the chassis:

Configuring an Ordinary Clock

The following sections describe how to configure the chassis as an ordinary clock.

Configuring a Master Ordinary Clock

Follow these steps to configure the chassis to act as a master ordinary clock.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. platformptp masterprte-only-enable
4. ptp clock {ordinary | boundary | e2e-transparent} domain domain-number
5. priority1 priorityvalue
6. priority2 priorityvalue
7. utc-offset value leap-second “date time” offset { -1 | 1 }
8. input [1pps] { R0 | R1 }
9. tod { R0 | R1 } { ubx | nmea | cisco | ntp }
10. clock-port port-name { master | slave } [ profile { g8265.1 } ]
11. Do one of the following:
   - transport ipv4 unicast interface interface-type interface-number [ negotiation ]
   - transport ethernet unicast [ negotiation ]
12. exit

8275.1 profile does not support QL-disabled mode on RSP3.
13. network-clock synchronization automatic
14. network-clock synchronization mode ql-enabled
15. Use one of the following options:
   - network-clock input-source priority controller {SONET | wanphy}
   - network-clock input-source priority external {R0 | R1} {10m | 2m}
   - network-clock input-source priority external {R0 | R1} {2048k | e1} {cas {120ohms | 75ohms | crc4}}
   - network-clock input-source priority external {R0 | R1} {2048k | e1} {crc4 | fas} {120ohms | 75ohms} {linecode {ami | hdb3}}
   - network-clock input-source priority external {R0 | R1} {t1 | d4 | esf | sf} {linecode {ami | b8zs}}
   - network-clock input-source priority interface type/slot/port

16. clock destination source-address | mac-address {bridge-domain bridge-domain-id} | interface interface-name
17. sync interval interval
18. announce interval interval
19. end
20. linecode {ami | b8zs | hdb3}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 platform ptp master prtc-only-enable</td>
<td>(Optional) Enable Master port deletion.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# platform ptp master prtc-only-enable</td>
<td></td>
</tr>
<tr>
<td>Step 4 ptp clock {ordinary</td>
<td>boundary</td>
</tr>
<tr>
<td>Example:</td>
<td>• ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.</td>
</tr>
<tr>
<td>Router(config)# ptp clock ordinary domain 0</td>
<td>• boundary—Terminates PTP session from Grandmaster and acts as PTP master to slaves downstream.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-tpclk)#</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>• e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at slave.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>priority1 <em>priorityvalue</em></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>priority2 <em>priorityvalue</em></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>utc-offset <em>value</em> leap-second <em>“date time”</em> offset {-1</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>input [1pps] {R0</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>tod {R0</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>clock-port</strong> port-name {master</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ptp-clk)# clock-port Master master</td>
<td><strong>Note</strong> Using a telecom profile requires that the clock have a domain number of 4–23.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td>Example:</td>
<td>• transport ipv4 unicast interface-type interface-number [negotiation]</td>
</tr>
<tr>
<td>Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation</td>
<td><strong>Note</strong> PTP redundancy is supported only on unicast negotiation mode.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>network-clock synchronization automatic</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# network-clock synchronization automatic</td>
<td><strong>Step 14</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# network-clock synchronization mode ql-enabled</td>
<td><strong>Step 15</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>• network-clock input-source priority controller {SONET</td>
</tr>
<tr>
<td>Router(config)# network-clock input-source priority controller {SONET</td>
<td>wanphy}</td>
</tr>
<tr>
<td>• network-clock input-source priority external {R0</td>
<td>R1} [2048k</td>
</tr>
<tr>
<td>• network-clock input-source priority external {R0</td>
<td>R1} [120ohms</td>
</tr>
<tr>
<td>• network-clock input-source priority interface type/slot/port</td>
<td><strong>Note</strong> This command must be configured before any input source.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# network-clock input-source 1 external R0 10m</td>
<td>Specifies the IP address or MAC address of a clock destination when the chassis is in PTP master mode.</td>
</tr>
<tr>
<td><strong>Step 16</strong> clock destination source-address</td>
<td>Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values, as follows:</td>
</tr>
<tr>
<td>mac-address {bridge-domain bridge-domain-id}</td>
<td>- 1—1 packet every 2 seconds</td>
</tr>
<tr>
<td>interface interface-name}</td>
<td>- 0—1 packet every second</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ptp-port)# clock-source 8.8.8.1</td>
<td>- -1—1 packet every 1/2 second, or 2 packets per second</td>
</tr>
<tr>
<td><strong>Step 17</strong> sync interval interval</td>
<td>- -2—1 packet every 1/4 second, or 4 packets per second</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ptp-port)# sync interval -4</td>
<td>- -3—1 packet every 1/8 second, or 8 packets per second</td>
</tr>
<tr>
<td><strong>Step 18</strong> announce interval interval</td>
<td>- -4—1 packet every 1/16 seconds, or 16 packets per second.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ptp-port)# announce interval 2</td>
<td>- -5—1 packet every 1/32 seconds, or 32 packets per second.</td>
</tr>
<tr>
<td></td>
<td>- -6—1 packet every 1/64 seconds, or 64 packets per second.</td>
</tr>
<tr>
<td></td>
<td>- -7—1 packet every 1/128 seconds, or 128 packets per second.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| • -2—1 packet every 1/4 second, or 4 packets per second  
• -3—1 packet every 1/8 second, or 8 packets per second | |

### Step 19

**End**

**Example:**

```
Router(config-ptp-port)# end
```

Exit configuration mode.

### Step 20

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

**Example:**

Router(config-controller)# linecode ami

Selects the line code type.

• **ami**—Specifies Alternate Mark Inversion (AMI) as the line code type. Valid for T1 and E1 controllers.

• **b8zs**—Specifies binary 8-zero substitution (B8ZS) as the line code type. Valid for sonet controller only. This is the default for T1 lines.

• **hdb3**—Specifies high-density binary 3 (hdb3) as the line code type. Valid for E1 controller only. This is the default for E1 lines.

---

**Example**

The following example shows that the utc-offset is configured before configuring the ToD to avoid a delay of 37 seconds between the master and slave clocks:

```
ptp clock ordinary domain 24
local-priority 1
priority2 128
utc-offset 37
tod R0 cisco
clock-port master-port-1 master profile g8275.1 local-priority 1
transport ethernet multicast interface Gig 0/0/1
```

---

### Configuring a Slave Ordinary Clock

Follow these steps to configure the chassis to act as a slave ordinary clock.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ptp clock {ordinary | boundary | e2e-transparent} domain domain-number [hybrid]**
4. **output [1pps] {R0 | R1} [offset offset-value] [pulse-width value]**
5. **tod {R0 | R1} {ubx | nmea | cisco | ntp}**
6. **clock-port port-name {master | slave} [profile {g8265.1}]**
7. Do one of the following:
   - `transport ipv4 unicast interface interface-type interface-number [negotiation]`
   - `transport ethernet unicast [negotiation]`

8. `clock source source-address | mac-address {bridge-domain bridge-domain-id} | interface interface-name {priority}`

9. `announce timeout value`

10. `delay-req interval interval`

11. `end`

12. `Router(config-controller)# linecode {ami | b8zs | hdb3}`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`ptp clock {ordinary</td>
<td>boundary</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.</td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# ptp clock ordinary domain 0</code></td>
<td>• boundary—Terminates PTP session from Grandmaster and acts as PTP master to slaves downstream.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at slave.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`output 1pps {R0</td>
<td>R1} [offset offset-value] [pulse-width value]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>Use R0 or R1 to specify the active RSP slot.</td>
</tr>
<tr>
<td></td>
<td><code>Router(config-tp-clk)# output 1pps R0 offset 200 pulse-width 20 μsec</code></td>
<td><strong>Note</strong>  Effective Cisco IOS XE Everest 16.6.1, the 1pps pulse bandwidth can be changed from the default value of 500 milliseconds to up to 20 microseconds.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>5</td>
<td>tod {R0</td>
<td>R1</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-ptp-clk)# tod R0 ntp</td>
<td>Note: The ToD port acts as an input port in case of Master clock and as an output port in case of Slave clock.</td>
</tr>
<tr>
<td>6</td>
<td>clock-port port-name {master</td>
<td>slave} [profile {g8265.1}]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>The profile keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes.</td>
</tr>
<tr>
<td></td>
<td>Router(config-ptp-clk)# clock-port Slave slave</td>
<td>Note: Using a telecom profile requires that the clock have a domain number of 4–23.</td>
</tr>
<tr>
<td>7</td>
<td>clock source source-address</td>
<td>Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.</td>
</tr>
<tr>
<td></td>
<td>mac-address</td>
<td>The negotiation keyword configures the chassis to discover a PTP master clock from all available PTP clock sources.</td>
</tr>
<tr>
<td></td>
<td>bridge-domain bridge-domain-id</td>
<td>Note: PTP redundancy is supported only on unicast negotiation mode.</td>
</tr>
<tr>
<td></td>
<td>interface interface-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[priority]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-ptp-port)# clock-source 8.8.8.1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>announce timeout value</td>
<td>Specifies the number of PTP announcement intervals before the session times out. Valid values are 1-10.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-ptp-port)# announce timeout 8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>delay-req interval interval</td>
<td>Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>The intervals are set using log base 2 values, as follows:</td>
</tr>
<tr>
<td></td>
<td>Router(config-ptp-port)# delay-req interval 1</td>
<td>• 3—1 packet every 8 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2—1 packet every 4 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—1 packet every 2 seconds</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>- 0 — 1 packet every second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-1 — 1 packet every 1/2 second, or 2 packets per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-2 — 1 packet every 1/4 second, or 4 packets per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-3 — 1 packet every 1/8 second, or 8 packets per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-4 — 1 packet every 1/16 seconds, or 16 packets per second.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-5 — 1 packet every 1/32 seconds, or 32 packets per second.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-6 — 1 packet every 1/64 seconds, or 64 packets per second.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-7 — 1 packet every 1/128 seconds, or 128 packets per second.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 11**

```
exit
```

Example:

```
Router(config-pty-port)# end
```

Exit configuration mode.

**Step 12**

```
Router(config-controller)# linecode {ami | b8zs | hdb3}
```

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 sonet 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.

---

**Configuring a Boundary Clock**

Follow these steps to configure the chassis to act as a boundary clock.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. Router(config)# ptp clock {ordinary | boundary | e2e-transparent} domain domain-number [hybrid]
4. time-properties persist value
5. `clock-port port-name {master | slave} [profile {g8265.1}]`
6. `transport ipv4 unicast interface interface-type interface-number [negotiation]`
7. `clock-source source-address [priority]`
8. `clock-port port-name {master | slave} [profile {g8265.1}]`
9. `transport ipv4 unicast interface interface-type interface-number [negotiation]`
10. `end`
11. `Router(config-controller)# linecode {ami | b8zs | hdb3}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Router(config)# ptp clock {ordinary</td>
<td>boundary</td>
</tr>
<tr>
<td>Example:</td>
<td>Configures the PTP clock. You can create the following clock types:</td>
</tr>
<tr>
<td></td>
<td>• ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.</td>
</tr>
<tr>
<td></td>
<td>• boundary—Terminates PTP session from Grandmaster and acts as PTP master to slaves downstream.</td>
</tr>
<tr>
<td></td>
<td>• e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at slave.</td>
</tr>
<tr>
<td><strong>Step 4</strong> time-properties persist value</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure time properties holdover time. Valid values are from 0 to 10000 seconds. The default value is 300 seconds.</td>
</tr>
<tr>
<td></td>
<td>When a master clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged. In case leap second midnight occurs when holdover timer is running, utc-offset value is updated based on leap59 or leap61 flags. This value is used as long as there are no PTP packets being received from the selected master. In case the selected master is sending announce packets, the time-properties advertised by master is used.</td>
</tr>
</tbody>
</table>
### Configuring Clocking and Timing

**Configuring a Boundary Clock**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5** | `clock-port port-name {master | slave} [profile {g8265.1}]` | Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP slave clock. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes. The **clock-port** command is used to set the clock port to PTP master or slave mode. The **profile** argument specifies the version of the G.8265.1 standard to use. The **port-name** argument specifies the name of the PTP port. Example:  
```
Router(config-ptp-clk)# clock-port SLAVE slave
```
**Note** Using a telecom profile requires that the clock have a domain number of 4–23. |
| **Step 6** | `transport ipv4 unicast interface interface-type interface-number [negotiation]` | Specifies the transport mechanism for clocking traffic. The **negotiation** keyword configures the chassis to discover a PTP master clock from all available PTP clock sources. The **transport** command is used to specify the transport mechanism for clocking traffic. The **ipv4**, **interface**, and **interface-type** arguments specify the transport mechanism. The **interface-number** argument specifies the interface number. Example:  
```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```
**Note** PTP redundancy is supported only on unicast negotiation mode. |
| **Step 7** | `clock-source source-address [priority]` | Specifies the address of a PTP master clock. You can specify a priority value as follows:  
- No priority value—Assigns a priority value of 0.  
- 1—Assigns a priority value of 1.  
- 2—Assigns a priority value of 2, the highest priority. Example:  
```
Router(config-ptp-port)# clock source 133.133.133.133
```
| **Step 8** | `clock-port port-name {master | slave} [profile {g8265.1}]` | Sets the clock port to PTP master or slave mode; in master mode, the port exchanges timing packets with PTP slave devices. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes. The **clock-port** command is used to set the clock port to PTP master or slave mode. The **profile** argument specifies the version of the G.8265.1 standard to use. The **port-name** argument specifies the name of the PTP port. Example:  
```
Router(config-ptp-port)# clock-port Master master
```
**Note** The master clock-port does not establish a clocking session until the slave clock-port is phase aligned.  
| **Step 9** | `transport ipv4 unicast interface interface-type interface-number [negotiation]` | Specifies the transport mechanism for clocking traffic. The **negotiation** keyword configures the chassis to discover a PTP master clock from all available PTP clock sources. The **transport** command is used to specify the transport mechanism for clocking traffic. The **ipv4**, **interface**, and **interface-type** arguments specify the transport mechanism. The **interface-number** argument specifies the interface number. Example:  
```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation
```
**Note** PTP redundancy is supported only on unicast negotiation mode. |
| **Step 10** | `end` | Exit configuration mode. Example:  
```
Router(config-ptp-port)# end
``` |
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-tp)-port)# end</td>
</tr>
</tbody>
</table>

**Step 11**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-controller)# linecode {ami</td>
<td>b8zs</td>
</tr>
</tbody>
</table>

- **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 sonet 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.

---

### What to do next

**Configuring a Transparent Clock**

Follow these steps to configure the chassis as an end-to-end transparent clock.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ptp clock {ordinary | boundary | e2e-transparent} domain domain-number [hybrid]`
4. `exit`
5. `Router(config-controller)# linecode {ami | b8zs | hdb3}`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter configuration mode.</td>
</tr>
</tbody>
</table>

**Note**

- The Cisco NCS 4206 Series Chassis does not support peer-to-peer transparent clock mode.
- The transparent clock ignores the domain number.
### Configuring a Hybrid Clock

The following sections describe how to configure the chassis to act as a hybrid clock.

#### Configuring a Hybrid Boundary Clock

Follow these steps to configure a hybrid clocking in boundary clock mode.

**Note**

When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same master clock.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ptp clock {boundary} domain domain-number [hybrid]`
4. `time-properties persist value`
5. `utc-offset value leap-second "date time" offset {-1 | 1}`
6. `min-clock-class value`
7. `clock-port port-name {master | slave} [profile {g8265.1}]`
8. `transport ipv4 unicast interface interface-type interface-number [negotiationsingle-hop]`
9. **clock-source** source-address [priority]
10. **clock-port** port-name {master | slave} [profile {g8265.1}]
11. **transport** ipv4 unicast interface interface-type interface-number [negotiation] /single-hop
12. exit
13. network-clock synchronization automatic
14. network-clock synchronization mode ql-enabled
15. Use one of the following options:
   
   • **network-clock input-source** priority controller {SONET | wanphy}
   
   • **network-clock input-source** priority external {R0 | R1} [10m | 2m]
   
   • **network-clock input-source** priority external {R0 | R1} [2048k | e1 | cas {120ohms | 75ohms | crc4}]
   
   • **network-clock input-source** priority external {R0 | R1} [2048k | e1 | crc4 | fas] {120ohms | 75ohms | linecode {ami | hdh3}}
   
   • **network-clock input-source** priority external {R0 | R1} [t1 | d4 | esf | sf] {linecode {ami | b8zs}}
   
   • **network-clock input-source** priority interface type/slot/port

16. **network-clock synchronization input-threshold** ql value
17. **network-clock hold-off** {0 | milliseconds}
18. platformptpmasteralways-on
19. platformptphybrid-bcdownstream-enable
20. end
21. Router(config-controller)# linecode {ami | b8zs | hdb3}

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ptp clock {boundary} domain domain-number [hybrid]</td>
<td>Configures the PTP clock. You can create the following clock types:</td>
</tr>
<tr>
<td>Example:</td>
<td>Note Hybrid mode is only supported with slave clock-ports; master mode is not supported.</td>
</tr>
<tr>
<td>Router(config)# ptp clock boundary domain 0 hybrid</td>
<td>• boundary—Terminates PTP session from Grandmaster and acts as PTP master to slaves downstream.</td>
</tr>
</tbody>
</table>
Configuring Clocking and Timing

---

**Command or Action**

**Purpose**

**Step 4**

- **time-properties persist value**

  **Example:**
  ```
  Router(config-ptp-clk)# time-properties persist 600
  ```

  *(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure time properties holdover time. Valid values are from 0 to 10000 seconds. The default value is 300 seconds.*

  When a master clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged. In case leap second midnight occurs when holdover timer is running, utc-offset value is updated based on leap59 or leap61 flags. This value is used as long as there are no PTP packets being received from the selected master. In case the selected master is sending announce packets, the time-properties advertised by master is used.

**Step 5**

- **utc-offset value leap-second "date time" offset {-1 | 1}**

  **Example:**
  ```
  Router(config-ptp-clk)# utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
  ```

  *(Optional) Starting with Cisco IOS-XE Release 3.18SP, the new utc-offset CLI is used to set the UTC offset value. Valid values are from 0-255. The default value is 36.*

  *(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure the current UTC offset, leap second event date and Offset value (+1 or -1). Leap second configuration will work only when the frequency source is locked and ToD was up before.*

  - "date time"—Leap second effective date in dd-mm-yyyy hh:mm:ss format.

**Step 6**

- **min-clock-class value**

  **Example:**
  ```
  Router(config-ptp-clk)# min-clock-class 157
  ```

  Sets the threshold clock-class value. This allows the PTP algorithm to use the time stamps from a upstream master clock, only if the clock-class sent by the master clock is less than or equal to the configured threshold clock-class.

  Valid values are from 0-255.

  **Note** Min-clock-class value is supported only for PTP with single master source configuration.

**Step 7**

- **clock-port port-name {master | slave} [profile {g8265.1}]**

  **Example:**
  ```
  Router(config-ptp-clk)# clock-port SLAVE slave
  ```

  Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP master clock.

  **Note** Hybrid mode is only supported with slave clock-ports; master mode is not supported.

  The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> transport ipv4 unicast interface interface-type interface-number [negotiationsingle-hop]</td>
<td>Specifies the transport mechanism for clocking traffic. <strong>negotiation</strong>—(Optional) configures the chassis to discover a PTP master clock from all available PTP clock sources. <strong>single-hop</strong>—(Optional) Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-PTP-port)# transport ipv4 unicast interface Loopback 0 negotiation</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Router(config-PTP-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> clock-source source-address [priority]</td>
<td>Specifies the address of a PTP master clock. You can specify a priority value as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-PTP-port)# clock source 133.133.133.133</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> clock-port port-name {master</td>
<td>slave} [profile {g8265.1}]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-PTP-port)# clock-port MASTER master</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> transport ipv4 unicast interface interface-type interface-number [negotiation] /single-hop]</td>
<td>Specifies the transport mechanism for clocking traffic. <strong>negotiation</strong>—(Optional) configures the chassis to discover a PTP master clock from all available PTP clock sources. <strong>single-hop</strong>—(Optional) Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-PTP-port)# transport ipv4 unicast interface Loopback 0 negotiation</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Router(config-PTP-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> exit</td>
<td>Exit clock-port configuration.</td>
</tr>
<tr>
<td><strong>Step 13</strong> network-clock synchronization automatic</td>
<td>Enables automatic selection of a clock source. <strong>Note</strong> This command must be configured before any input source.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# network-clock synchronization automatic</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Enables automatic selection of a clock source based on quality level (QL).</td>
</tr>
<tr>
<td><code>network-clock synchronization mode ql-enabled</code></td>
<td>This command is disabled by default.</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>Use one of the following options:</td>
</tr>
<tr>
<td>`network-clock input-source priority controller {SONET</td>
<td>wanphy}`</td>
</tr>
<tr>
<td>`network-clock input-source priority external {R0</td>
<td>R1} [10m</td>
</tr>
<tr>
<td>`network-clock input-source priority external {R0</td>
<td>R1} [2048k</td>
</tr>
<tr>
<td>`network-clock input-source priority external {R0</td>
<td>R1} [2048k</td>
</tr>
<tr>
<td><code>network-clock input-source priority interface type/slot/port</code></td>
<td>- (Optional) To nominate Ethernet interface as network clock input source.</td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td>(Optional) Starting with Cisco IOS-XE Release 3.18SP, this new CLI is used to set the threshold QL value for the input frequency source. The input frequency source, which is better than or equal to the configured threshold QL value, will be selected to recover the frequency. Otherwise, internal clock is selected.</td>
</tr>
<tr>
<td><code>network-clock synchronization input-threshold ql value</code></td>
<td>(Optional) Configures a global hold-off timer specifying the amount of time that the chassis waits when a synchronous Ethernet clock source fails before taking action.</td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td>You can also specify a hold-off value for an individual interface using the <code>network-clock hold-off</code> command in interface mode.</td>
</tr>
<tr>
<td>`network-clock hold-off {0</td>
<td>milliseconds}`</td>
</tr>
<tr>
<td><strong>Step 18</strong></td>
<td>(Optional) Keeps the master port up all the time. So, when the frequency source has acceptable QL, the egress packets are sent to the downstream slaves even when the master port is not phase aligned.</td>
</tr>
<tr>
<td><code>platform ptp master always-on</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Clocking and Timing

#### Configuring a Hybrid Ordinary Clock

Follow these steps to configure a hybrid clocking in ordinary clock slave mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 19</strong></td>
<td>(Optional) Enables bust mode. When the difference between the forward timestamp of the previous packet and current packet is greater than 100ns, such timestamps are not provided to the APR. Due to this setting, the APR does not see unexpected and random time jumps in two sequential timestamps of the same PTP message-types. The same applies for the reverse path timestamps as well.</td>
</tr>
<tr>
<td>platform ptp hybrid-bc downstream-enable</td>
<td>Example: <code>Router(config)# platform ptp hybrid-bc downstream-enable</code></td>
</tr>
<tr>
<td><strong>Step 20</strong></td>
<td>Exit configuration mode.</td>
</tr>
<tr>
<td>end</td>
<td>Example: <code>Router(config)# end</code></td>
</tr>
<tr>
<td><strong>Step 21</strong></td>
<td>Selects the linecode type.</td>
</tr>
</tbody>
</table>
| Router(config-controller)# linecode {ami | b8zs | hdb3} | - **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 sonet 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. |

---

### Configuring a Hybrid Ordinary Clock

When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same master clock.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ptp clock {ordinary | boundary | c2e-transparent} domain domain-number [hybrid]
4. output [1pps] {R0 | R1} [offset offset-value] [pulse-width value]
5. tod {R0 | R1} {ubx | nmea | cisco | ntp}
6. clock-port port-name {master | slave} [profile {g8265.1}]
7. transport ipv4 unicast interface interface-type interface-number [negotiation]
8. clock-source source-address [priority]
9. exit
10. network-clock synchronization automatic
11. network-clock synchronization mode q1-enabled
12. Use one of the following options:
• network-clock input-source <priority> controller {SONET | wanphy}
• network-clock input-source <priority> external {R0 | R1} [10m | 2m]
• network-clock input-source <priority> external {R0 | R1} [2048k | e1 {cas {120ohms | 75ohms | crc4}}]
• network-clock input-source <priority> external {R0 | R1} [2048k | e1 {crc4 | fas} {120ohms | 75ohms} {linecode {ami | hdb3}}]
• network-clock input-source <priority> external {R0 | R1} [t1 {d4 | esf | sf} {linecode {ami | b8zs}}]
• network-clock input-source <priority> interface <type/slot/port>

13. network-clock hold-off {0 | milliseconds}
14. end
15. Router(config-controller)# linecode {ami | b8zs | hdb3}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
|      | Example:          |  
|      | Router> enable    |  
| 2    | configure terminal| Enter configuration mode. |
|      | Example:          |  
|      | Router# configure terminal |  
| 3    | ptp clock {ordinary | boundary | e2e-transparent} domain domain-number [hybrid] | Configures the PTP clock. You can create the following clock types:  
|      | Example:          |  
|      | Router(config)# ptp clock ordinary domain 0 hybrid |  
| 4    | output [1pps] {R0 | R1} [offset offset-value] [pulse-width value] | Enables Precision Time Protocol input 1PPS using a 1PPS input port. |
|      | Example:          | Use R0 or R1 to specify the active RSP slot. |
|      | Router(config-tp-clk)# output 1pps R0 offset 200 pulse-width 20 μsec |  
|      | Note              | Effective Cisco IOS XE Everest 16.6.1, the 1pps pulse bandwidth can be changed from the default value of 500 milliseconds to up to 20 microseconds. |

Note: Hybrid mode is only supported with slave clock-ports; master mode is not supported.
<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tod {R0</td>
<td>R1} {ubx</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ptp-clk)# tod R0 ntp</td>
<td>The ToD port acts as an input port in case of Master clock and as an output port in case of Slave clock.</td>
</tr>
</tbody>
</table>

| Step 6 | clock-port port-name {master | slave} {profile {g8265.1}} | Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP master clock. |
| Example: | Router(config-ptp-clk)# clock-port SLAVE slave | Hybrid mode is only supported with slave clock-ports; master mode is not supported. |

| Step 7 | transport ipv4 unicast interface interface-type interface-number [negotiation/ | Specifies the transport mechanism for clocking traffic. |
| Example: | Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation | The negotiation keyword configures the router to discover a PTP master clock from all available PTP clock sources. |
|         |         | PTP redundancy is supported only on unicast negotiation mode. |

| Step 8 | clock-source source-address [priority] | Specifies the address of a PTP master clock. You can specify a priority value as follows: |
| Example: | Router(config-ptp-port)# clock source 133.133.133.133 | • No priority value—Assigns a priority value of 0. |
|         |         | • 1—Assigns a priority value of 1. |
|         |         | • 2—Assigns a priority value of 2, the highest priority. |

| Step 9 | exit | Exit clock-port configuration. |
| Example: | Router(config-ptp-port)# exit | |

<p>| Step 10 | network-clock synchronization automatic | Enables automatic selection of a clock source. |
| Example: | Router(config-ptp-clk)# network-clock synchronization automatic | This command must be configured before any input source. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 11**  
*network-clock synchronization mode ql-enabled*  
Example:  
```
Router(config-ptp-clk)# network-clock synchronization mode ql-enabled
```
| Enables automatic selection of a clock source based on quality level (QL). |
| **Note**  
This command is disabled by default. |
| For more information about this command, see Configuring Clocking and Timing, on page 31 |

| Step 12 |  
Use one of the following options:  
- *network-clock input-source <priority> controller {SONET | wanphy}*  
- *network-clock input-source <priority> external {R0 | R1} [10m | 2m]*  
- *network-clock input-source <priority> external {R0 | R1} [2048k | e1 {cas {120ohms | 75ohms | crc4} | fas} | 120ohms | 75ohms} {linecode {ami | hdb3}}]*  
- *network-clock input-source <priority> external {R0 | R1} [2048k | e1 {crc4 | fas} | 120ohms | 75ohms} {linecode {ami | b8zs}}]*  
- *network-clock input-source <priority> interface <type/slot/port>*  
|  
**Example:**  
```
Router(config)# network-clock input-source 1 external R0 10m
```
|  
(Optional) To nominate SDH or SONET controller as network clock input source.  
(Optional) To nominate 10MHz port as network clock input source.  
(Optional) To nominate BITS port as network clock input source in e1 mode.  
(Optional) To nominate BITS port as network clock input source in t1 mode.  
(Optional) To nominate BITS port as network clock input source.  
Optional to nominate Ethernet interface as network clock input source. |

| Step 13 |  
*network-clock hold-off {0 | milliseconds}*  
Example:  
```
Router(config-ptp-clk)# network-clock hold-off 0
```
| (Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action. |
| **Note**  
You can also specify a hold-off value for an individual interface using the *network-clock hold-off* command in interface mode. |
| For more information about this command, see Configuring Clocking and Timing, on page 31 |

| Step 14 |  
*end*  
Example:  
```
Router(config-ptp-clk)# end
```
| Exit configuration mode. |

| Step 15 |  
*Router(config-controller)# linecode {ami | b8zs | hdb3}*  
Example:  
```
```
| Selects the linecode type.  
- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers. |
### Configuring PTP Redundancy

The following sections describe how to configure PTP redundancy on the chassis:

#### Configuring PTP Redundancy in Slave Clock Mode

Follow these steps to configure clocking redundancy in slave clock mode:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. `ptp clock {ordinary | boundary | e2e-transparent} domain domain-number [hybrid]`
4. `clock-port port-name {master | slave} [profile {g8265.1}]`
5. `transport ipv4 unicast interface interface-type interface-number [negotiation] [single-hop]`
6. `clock-source source-address [priority]`
7. `clock-source source-address [priority]`
8. `clock-source source-address [priority]`
9. end
10. Router(config-controller)# linecode {ami | b8zs | hdb3}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `ptp clock {ordinary</td>
<td>boundary</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>- <code>ordinary</code>—A 1588 clock with a single PTP port that can operate in Master or Slave mode.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>router(config)# ptp clock ordinary domain 0</code></td>
<td>Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP master clock. The <code>profile</code> keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes. <strong>Note</strong> Using a telecom profile requires that the clock have a domain number of 4–23.</td>
</tr>
</tbody>
</table>
| **Step 4** `clock-port port-name {master | slave} [profile {g8265.1}]` | **Example:**
```
routing(config-ptp-clk)# clock-port SLAVE slave
```
Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP master clock. The `profile` keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23. |
| **Step 5** `transport ipv4 unicast interface interface-type interface-number [negotiation] [single-hop]` | **Example:**
```
routing(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```
Specifies the transport mechanism for clocking traffic. **Note** PTP redundancy is supported only on unicast negotiation mode. **Single-hop**—(Optional) It ensures that the PTP node communicates only with the adjacent nodes. |
| **Step 6** `clock-source source-address [priority]` | **Example:**
```
routing(config-ptp-port)# clock source 133.133.133.133 1
```
Specifies the address of a PTP master clock. You can specify a priority value as follows:
- **No priority value**—Assigns a priority value of 0.
- **1**—Assigns a priority value of 1.
- **2**—Assigns a priority value of 2, the highest priority. |
| **Step 7** `clock-source source-address [priority]` | **Example:**
```
routing(config-ptp-port)# clock source 133.133.133.133 2
```
Specifies the address of an additional PTP master clock; repeat this step for each additional master clock. You can configure up to 3 master clocks. |
| **Step 8** `clock-source source-address [priority]` | **Example:**
```
routing(config-ptp-port)# clock source 133.133.133.134
```
Specifies the address of an additional PTP master clock; repeat this step for each additional master clock. You can configure up to 3 master clocks. |
| **Step 9** `end` | **Example:**
```
```
Exit configuration mode. |
Configuring PTP Redundancy in Boundary Clock Mode

Follow these steps to configure clocking redundancy in boundary clock mode:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ptp clock {ordinary | boundary | e2e-transparent} domain domain-number`
4. `clock-port port-name {master | slave} [profile {g8265.1}]`
5. `transport ipv4 unicast interface interface-type interface-number [negotiation] [single-hop]`
6. `clock-source source-address [priority]`
7. `clock-source source-address [priority]`
8. `clock-source source-address [priority]`
9. `clock-port port-name {master | slave} [profile {g8265.1}]`
10. `transport ipv4 unicast interface interface-type interface-number [negotiation] [single-hop]`
11. `end`
12. `Router(config-controller)# linecode {ami | b8zs | hdb3}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the PTP clock. You can create the following clock types:</td>
</tr>
<tr>
<td>`ptp clock {ordinary</td>
<td>boundary</td>
</tr>
</tbody>
</table>

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 sonet 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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Example:** | • ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.  
• boundary—Terminates PTP session from Grandmaster and acts as PTP master to slaves downstream.  
• e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at slave. |
| **Step 4** |  
**clock-port** *port-name* {master | slave} [profile {g8265.1}]  
*Example:*  
Router(config-ptp-clk)# clock-port SLAVE slave  
Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP master clock.  
The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes.  
**Note** Using a telecom profile requires that the clock have a domain number of 4–23. |
| **Step 5** |  
**transport ipv4 unicast interface** *interface-type* *interface-number* [negotiation] [single-hop]  
*Example:*  
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation  
Specifications the transport mechanism for clocking traffic.  
• **negotiation**—(Optional) Configures the chassis to discover a PTP master clock from all available PTP clock sources.  
**Note** PTP redundancy is supported only on unicast negotiation mode.  
• **single-hop**—(Optional) Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes. |
| **Step 6** |  
**clock-source** *source-address* [priority]  
*Example:*  
Router(config-ptp-port)# clock source 133.133.133.133 1  
Specifies the address of a PTP master clock. You can specify a priority value as follows:  
• No priority value—Assigns a priority value of 0.  
• 1—Assigns a priority value of 1.  
• 2—Assigns a priority value of 2, the highest priority. |
| **Step 7** |  
**clock-source** *source-address* [priority]  
*Example:*  
Router(config-ptp-port)# clock source 133.133.133.134 2  
Specifies the address of an additional PTP master clock; repeat this step for each additional master clock. You can configure up to 3 master clocks. |
| **Step 8** |  
**clock-source** *source-address* [priority]  
*Example:*  
Router(config-ptp-port)# clock source 133.133.133.135  
Specifies the address of an additional PTP master clock; repeat this step for each additional master clock. You can configure up to 3 master clocks. |
### Configuring Clocking and Timing

#### Synchronizing the System Time to a Time-of-Day Source

The following sections describe how to synchronize the system time to a time of day (ToD) clock source.

### Synchronizing the System Time to a Time-of-Day Source (Master Mode)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 9** | clock-port *port-name {master | slave} [profile {g8265.1}]
Example:  
Router(config-pty-port)# clock-port MASTER master | Specifies the address of a PTP master clock.  
The *profile* keyword configures the clock to use the  
G.8265.1 recommendations for establishing PTP sessions,  
determining the best master clock, handling SSM, and  
mapping PTP classes.  
Note Using a telecom profile requires that the clock  
have a domain number of 4–23. |
| **Step 10** | transport ipv4 unicast interface *interface-type  
interface-number [negotiation] /single-hop
Example:  
Router(config-pty-port)# transport ipv4 unicast  
interface Loopback 1 negotiation single-hop | Specifies the transport mechanism for clocking traffic.  
• *negotiation*—(Optional) Configures the chassis to  
discover a PTP master clock from all available PTP  
clock sources.  
Note PTP redundancy is supported only on unicast  
negotiation mode.  
• *single-hop*—(Optional) Must be configured if  
Hop-by-Hop PTP ring topology is used. It ensures  
that the PTP node communicates only with the  
adjacent nodes. |
| **Step 11** | end
Example:  
Router(config-pty-port)# end | Exit configuration mode. |
| **Step 12** | Router(config-controller)# linecode {ami | b8zs | hdb3} | 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 sonet 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. |

---

**Synchronizing the System Time to a Time-of-Day Source**

The following sections describe how to synchronize the system time to a time of day (ToD) clock source.

**Synchronizing the System Time to a Time-of-Day Source (Master Mode)**

![Note](https://en.wikipedia.org/wiki/Note)

**Note**  
System time to a ToD source (Master Mode) can be configured only when PTP master is configured. See  
**Configuring a Master Ordinary Clock**, on page 44. Select any one of the four available ToD format; cisco,  
nmea, ntp or ubx.10m must be configured as network clock input source.
Follow these steps to configure the system clock to a ToD source in master mode.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `tod-clock input-source priority {gps {R0 | R1} | ptp domain domain}`
4. `exit`
5. `Router(config-controller)# linecode {ami | b8zs | hdb3}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | `enable`          | Enables privileged EXEC mode.  
    | Example:          | • Enter your password if prompted.  
    | Router> enable    |         |
| 2    | `configure terminal` | Enter configuration mode.  
    | Example:          |         |
|      | Router# configure terminal |      |
| 3    | `tod-clock input-source priority {gps {R0 | R1} | ptp domain domain}` | In master mode, specify a GPS port connected to a ToD source.  
    | Example:          |         |
|      | Router(config)# TOD-clock 2 gps R0/R1 |      |
| 4    | `exit`            | Exit configuration mode.  
    | Example:          |         |
|      | Router(config)# exit |      |
| 5    | `Router(config-controller)# linecode {ami | b8zs | hdb3}` | 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 sonet 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.  
    | |
Synchronizing the System Time to a Time-of-Day Source (Slave Mode)

Note
System time to a ToD source (Slave Mode) can be configured only when PTP slave is configured. See Configuring a Slave Ordinary Clock, on page 49.

Follow these steps to configure the system clock to a ToD source in slave mode. In slave mode, specify a PTP domain as a ToD input source.

SUMMARY STEPS

1. enable
2. configure terminal
3. tod-clock input-source priority {gps {R0 | R1} | ptp domain domain}
4. Router(config)# end
5. Router(config-controller)# linecode {ami | b8zs | hdb3}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 tod-clock input-source priority {gps {R0</td>
<td>R1}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# TOD-clock 10 ptp domain 0</td>
<td></td>
</tr>
<tr>
<td>Step 4 Router(config)# end</td>
<td>Exit configuration mode.</td>
</tr>
<tr>
<td>Step 5 Router(config-controller)# linecode {ami</td>
<td>b8zs</td>
</tr>
<tr>
<td></td>
<td>• ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.</td>
</tr>
<tr>
<td></td>
<td>• b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.</td>
</tr>
<tr>
<td></td>
<td>• hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.</td>
</tr>
</tbody>
</table>
Configuring Synchronous Ethernet ESMC and SSM

Synchronous Ethernet is an extension of Ethernet designed to provide the reliability found in traditional SONET/SDH and T1/E1 networks to Ethernet packet networks by incorporating clock synchronization features. The supports the Synchronization Status Message (SSM) and Ethernet Synchronization Message Channel (ESMC) for synchronous Ethernet clock synchronization.

The following sections describe ESMC and SSM support on the router.

Configuring Synchronous Ethernet ESMC and SSM

Follow these steps to configure ESMC and SSM on the router.

SUMMARY STEPS

1. enable
2. configure terminal
3. network-clock synchronization automatic
4. network-clock eec {1 | 2}
5. network-clock synchronization ssm option {1 | 2 | GEN1 | GEN2}
6. Use one of the following options:
   • network-clock input-source priority controller {SONET | wanphy}
   • network-clock input-source priority external {R0 | R1 | 10m | 2m}
   • network-clock input-source priority external {R0 | R1 | 2048k | e1 | cas | 120ohms | 75ohms | crc4 | fas}
   • network-clock input-source priority external {R0 | R1 | 2048k | e1 | 120ohms | 75ohms | linecode | ami | hdb3}
   • network-clock input-source priority external {R0 | R1 | t1 | d4 | esf | sf | linecode | ami | b8zs}
   • network-clock input-source priority interface type/slot/port
7. network-clock synchronization mode ql-enabled
8. network-clock hold-off {0 | milliseconds}
9. network-clock wait-to-restore seconds
10. network-clock revertive
11. esmc process
12. network-clock external slot/card/port hold-off {0 | milliseconds}
13. network-clock quality-level {tx | rx} value {controller | E1 | BITS} slot/card/port | external {2m | 10m | 2048k | t1 | e1}
14. interface type number
15. synchronous mode
16. network-clock source quality-level value {tx | rx}
17. esmc mode {ql-disabled | tx | rx} value
18. network-clock hold-off {0 | milliseconds}
19. network-clock wait-to-restore seconds
20. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
|      | Example:          | - Enter your password if prompted. |
|      | Router> enable    |         |
| 2    | configure terminal| Enters global configuration mode. |
|      | Example:          |         |
|      | Router# configure terminal | |
| 3    | network-clock synchronization automatic | Enables the network clock selection algorithm. This command disables the Cisco-specific network clock process and turns on the G.781-based automatic clock selection process. |
|      | Example:          |         |
|      | Router(config)# network-clock synchronization automatic | |
| 4    | network-clock eec \{1 | 2\} | Specifies the Ethernet Equipment Clock (EEC) type. Valid values are  
|      | Example:          | - 1—ITU-T G.8262 option 1 (2048)  
|      | Router(config)# network-clock eec 1 | - 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544) |
| 5    | network-clock synchronization ssm option \{1 | 2 | GEN1 | GEN2\} | Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command:  
|      | Example:          | - Option 1 refers to G.781 synchronization option 1, which is designed for Europe. This is the default value.  
|      | Router(config)# network-clock synchronization ssm option 2 GEN2 | - Option 2 refers to G.781 synchronization option 2, which is designed for the United States.  
|      |                  | - GEN1 specifies option 2 Generation 1 synchronization.  
|      |                  | - GEN2 specifies option 2 Generation 2 synchronization.  
| 6    | Use one of the following options: | (Optional) To nominate SDH or SONET controller as network clock input source.  
|      | - network-clock input-source priority controller \{SONET | wanphy\} | (Optional) To nominate 10Mhz port as network clock input source.  
|      | - network-clock input-source priority external \{R0 | R1\} \{10m | 2m\} | (Optional) To nominate BITS port as network clock input source in e1 mode.  
|      | - network-clock input-source priority external \{R0 | R1\} \{2048k | e1 \{cas \{120ohms | 75ohms | crc4\}\} | (Optional) To nominate BITS port as network clock input source in e1 mode.  

---

*Note: This command must be configured before any input source.*
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• network-clock input-source priority external {R0</td>
<td>R1} [2048k</td>
</tr>
<tr>
<td>• network-clock input-source priority external {R0</td>
<td>R1} [t1</td>
</tr>
<tr>
<td>• network-clock input-source priority interface type/slot/port</td>
<td>• (Optional) To nominate PTP as network clock input source.</td>
</tr>
</tbody>
</table>

Example:

Router(config)# network-clock input-source 1 external R0 10m

Step 7

network-clock synchronization mode ql-enabled

Example:

Router(config)# network-clock synchronization mode ql-enabled

Enables automatic selection of a clock source based on quality level (QL).

Note This command is disabled by default.

Step 8

network-clock hold-off {0 | milliseconds}

Example:

Router(config)# network-clock hold-off 0

(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

Note You can also specify a hold-off value for an individual interface using the network-clock hold-off command in interface mode.

Step 9

network-clock wait-to-restore seconds

Example:

Router(config)# network-clock wait-to-restore 70

(Optional) Configures a global wait-to-restore timer for synchronous Ethernet clock sources. The timer specifies how long the router waits before including a restored clock source in the clock selection process.

Valid values are 0 to 86400 seconds. The default value is 300 seconds.

Note You can also specify a wait-to-restore value for an individual interface using the network-clock wait-to-restore command in interface mode.

Step 10

network-clock revertive

Example:

Router(config)# network-clock revertive

(Optional) Sets the router in revertive switching mode when recovering from a failure. To disable revertive mode, use the no form of this command.

Step 11

esmc process

Example:

Router(config)# esmc process

Enables the ESMC process globally.
| Step 12 | network-clock external slot/card/port hold-off {0 | milliseconds} | Overrides the hold-off timer value for the external interface. |
|---|---|---|
| **Example:** | | |
| | Router(config)# network-clock external 0/1/0 hold-off 0 | |

| Step 13 | network-clock quality-level {tx | rx} value {controller [E1 | BITS] slot/card/port | external [2m | 10m | 2048k | t1 | e1] } | Specifies a quality level for a line or external clock source. The available quality values depend on the G.781 synchronization settings specified by the network-clock synchronization ssm option command: |
|---|---|---|
| **Example:** | | |
| | Router(config)# network-clock quality-level rx qL-pRC external R0 e1 cas crc4 | |

<table>
<thead>
<tr>
<th>Step 14</th>
<th>interface type number</th>
<th>Enters interface configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface GigabitEthernet 0/0/1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 15</th>
<th>synchronous mode</th>
<th>Configures the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# synchronous mode</td>
<td></td>
</tr>
</tbody>
</table>

| Step 16 | network-clock source quality-level value {tx | rx} | Applies quality level on sync E interface. The available quality values depend on the G.781 synchronization settings specified by the network-clock synchronization ssm option command: |
|---|---|---|
| **Example:** | | |
| | Router(config-if)# network-clock source quality-level QL-PrC tx | |

| Step 17 | esmc mode [ql-disabled | tx | rx] value | Enables the ESMC process at the interface level. The no form of the command disables the ESMC process. |
|---|---|---|
| **Example:** | | |
### Managing Clock Source Selection

The following sections describe how to manage the selection on the chassis:

#### Specifying a Clock Source

The following sections describe how to specify a synchronous Ethernet clock source during the clock selection process:

#### Selecting a Specific Clock Source

To select a specific interface as a synchronous Ethernet clock source, use the network-clock switch manual command in global configuration mode.

**Note**

The new clock source must be of higher quality than the current clock source; otherwise, the chassis does not select the new clock source.
**Specifying a Clock Source**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`network-clock switch manual external R0</td>
<td>R1 ```{E1 {crc4</td>
</tr>
<tr>
<td><code>Router# network-clock switch manual external r0 e1 crc4</code></td>
<td></td>
</tr>
<tr>
<td>`network-clock clear switch [t0</td>
<td>external slot/card/port [10m</td>
</tr>
<tr>
<td><code>Router# network-clock clear switch t0</code></td>
<td></td>
</tr>
</tbody>
</table>

**Forcing a Clock Source Selection**

To force the chassis to use a specific synchronous Ethernet clock source, use the `network-clock switch force` command in global configuration mode.

**Note**

This command selects the new clock regardless of availability or quality.

**Note**

Forcing a clock source selection overrides a clock selection using the `network-clock switch manual command`.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`network-clock switch force external R0</td>
<td>R1 ```{E1 {crc4</td>
</tr>
<tr>
<td><code>Router# network-clock switch force r0 e1 crc4</code></td>
<td></td>
</tr>
<tr>
<td>`network-clock clear switch [t0</td>
<td>external slot/card/port [10m</td>
</tr>
<tr>
<td><code>Router# network-clock clear switch t0</code></td>
<td></td>
</tr>
</tbody>
</table>

**Disabling Clock Source Specification Commands**

To disable a `network-clock switch manual` or `network-clock switch force` configuration and revert to the default clock source selection process, use the `network-clock clear switch` command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`network-clock clear switch [t0</td>
<td>external slot/card/port [10m</td>
</tr>
<tr>
<td><code>Router# network-clock clear switch t0</code></td>
<td></td>
</tr>
</tbody>
</table>
Disabling a Clock Source

The following sections describe how to manage the synchronous Ethernet clock sources that are available for clock selection:

### Locking Out a Clock Source

To prevent the chassis from selecting a specific synchronous Ethernet clock source, use the `network-clock set lockout` command in global configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`network-clock set lockout {interface interface_name slot/card/port</td>
<td>external</td>
</tr>
</tbody>
</table>

Router# network-clock set lockout interface GigabitEthernet 0/0/0

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`network-clock clear lockout {interface interface_name slot/card/port</td>
<td>external</td>
</tr>
</tbody>
</table>

Router# network-clock clear lockout interface GigabitEthernet 0/0/0

### Restoring a Clock Source

To restore a clock in a lockout condition to the pool of available clock sources, use the `network-clock clear lockout` command in global configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`network-clock clear lockout {interface interface_name slot/card/port</td>
<td>external</td>
</tr>
</tbody>
</table>

Router# network-clock clear lockout interface GigabitEthernet 0/0/0

### Verifying the Configuration

You can use the following commands to verify a clocking configuration:

- `show esmc`—Displays the ESMC configuration.
- `show esmc detail`—Displays the details of the ESMC parameters at the global and interface levels.
- `show network-clock synchronization`—Displays the chassis clock synchronization state.

---

Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE Fuji 16.9.x
• show network-clock synchronization detail—Displays the details of network clock synchronization parameters at the global and interface levels.
• show ptp clock dataset
• show ptp port dataset
• show ptp clock running
• show platform software ptpd statistics
• show platform ptp all
• show platform ptp tod all

Troubleshooting

Table 11: SyncE Debug Commands, on page 79 list the debug commands that are available for troubleshooting the SyncE configuration on the chassis:

⚠️ Caution
We recommend that you do not use debug commands without TAC supervision.

<table>
<thead>
<tr>
<th>Debug Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug platform network-clock</td>
<td>Debugs issues related to the network clock including active-standby selection, alarms, and OOR messages.</td>
</tr>
<tr>
<td>debug network-clock</td>
<td>Debugs issues related to network clock selection.</td>
</tr>
<tr>
<td>debug esmc error</td>
<td>These commands verify whether the ESMC packets are transmitted and received with proper quality-level values.</td>
</tr>
<tr>
<td>debug esmc event</td>
<td></td>
</tr>
<tr>
<td>debug esmc packet interface interface-name</td>
<td></td>
</tr>
<tr>
<td>debug esmc packet rx interface interface-name</td>
<td></td>
</tr>
<tr>
<td>debug esmc packet tx interface interface-name</td>
<td></td>
</tr>
</tbody>
</table>

Table 12: Troubleshooting Scenarios, on page 79 provides the information about troubleshooting your configuration

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Clock selection | • Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command.  
• Ensure that the nonrevertive configurations are in place.  
• Reproduce the issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm commands. Contact Cisco Technical Support if the issue persists. |
### Problem | Solution
---|---
Incorrect QL values | • Ensure that there is no framing mismatch with the SSM option.  
• Reproduce the issue using the debug network-clock errors and debug network-clock event commands.

Alarms | • Reproduce the issue using the debug platform network-clock command enabled in the RSP. Alternatively, enable the debug network-clock event and debug network-clock errors commands.

Incorrect clock limit set or queue limit disabled mode | • Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command.  
• Use the `show network-clock synchronization` command to confirm if the system is in revertive mode or non-revertive mode and verify the non-revertive configurations.  
• Reproduce the current issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm RSP commands.

Incorrect QL values when you use the `show network-clock synchronization detail` command. | • Use the `network clock synchronization SSM (option 1 | option 2)` command to confirm that there is no framing mismatch. Use the `show run interface` command to validate the framing for a specific interface. For the SSM option 1, framing should be SDH or E1, and for SSM option 2, it should be T1.  
• Reproduce the issue using the debug network-clock errors and debug network-clock event RSP commands.

---

**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.

### Configuration Examples

This section contains sample configurations for clocking features on the chassis.

**Note**

This section contains partial chassis configurations intended to demonstrate a specific feature.
Ordinary Clock—Slave

ptp clock ordinary domain 0
clock-port Slave slave
transport ipv4 unicast interface loopback 0 negotiation
clock-source 8.8.8.1
announce timeout 7
delay-req interval 100

Ordinary Clock—Slave Mode (Ethernet)

ptp clock ordinary domain 0
clock-port Slave slave
transport ethernet unicast
clock-source 1234.5678.90ab bridge-domain 2 5

Ordinary Clock—Master

ptp clock ordinary domain 0
clock-port Master master
transport ipv4 unicast interface loopback 0 negotiation

Ordinary Clock—Master (Ethernet)

ptp clock ordinary domain 0
clock-port Master master
transport ethernet unicast
clock destination interface GigabitEthernet0/0/1

Unicast Configuration—Slave Mode

ptp clock ordinary domain 0
clock-port Slave slave
transport ipv4 unicast interface loopback 0
clock-source 8.8.8.1

Unicast Configuration—Slave Mode (Ethernet)

ptp clock ordinary domain 0
clock-port Slave slave
transport ethernet unicast
clock source 1234.5678.90ab bridge-domain 5 2

Unicast Configuration—Master Mode

ptp clock ordinary domain 0
clock-port Master master
transport ipv4 unicast interface loopback 0
clock-destination 8.8.8.2
sync interval 1
announce interval 2
Unicast Configuration—Master Mode (Ethernet)

```
ptp clock ordinary domain 0
  clock-port Master master
  transport ethernet unicast
    clock destination 1234.5678.90ab bridge-domain 5
```
clock-port SLAVE slave
  transport ipv4 unicast interface Loopback0 negotiation
  clock source 133.133.133.133
  clock-port MASTER master
  transport ipv4 unicast interface Loopback1 negotiation
Network-clock input-source 10 interface gigabitEthernet 0/4/0

**Hybrid Clock—Slave**

ptp clock ordinary domain 0 hybrid
  clock-port SLAVE slave
    transport ipv4 unicast interface Loopback 0 negotiation
    clock source 133.133.133.133
Network-clock input-source 10 interface gigabitEthernet 0/4/0

**PTP Redundancy—Slave**

ptp clock ordinary domain 0
  clock-port SLAVE slave
    transport ipv4 unicast interface Loopback 0 negotiation
    clock source 133.133.133.133 1
    clock source 55.55.55.55 2
    clock source 5.5.5.5

**PTP Redundancy—Boundary**

ptp clock boundary domain 0
  clock-port SLAVE slave
    transport ipv4 unicast interface Loopback 0 negotiation
    clock source 133.133.133.133 1
    clock source 55.55.55.55 2
    clock source 5.5.5.5
  clock-port MASTER master
    transport ipv4 unicast interface Lo1 negotiation

**Hop-By-Hop PTP Redundancy—Slave**

ptp clock ordinary domain 0
  clock-port SLAVE slave
    transport ipv4 unicast interface Loopback 0 negotiation single-hop
    clock source 133.133.133.133 1
    clock source 55.55.55.55 2
    clock source 5.5.5.5

**Hop-By-Hop PTP Redundancy—Boundary**

ptp clock boundary domain 0
  clock-port SLAVE slave
    transport ipv4 unicast interface Loopback 0 negotiation single-hop
    clock source 133.133.133.133 1
    clock source 55.55.55.55 2
    clock source 5.5.5.5
clock-port MASTER master
transport ipv4 unicast interface Lo1 negotiation single-hop

Time of Day Source—Master

TOD-clock 10 gps R0/R1

Time of Day Source—Slave

TOD-clock 10 ptp domain 0

Clock Selection Parameters

network-clock synchronization automatic
network-clock synchronization mode QL-enabled
network-clock input-source 1 ptp domain 3

ToD/1PPS Configuration—Master

network-clock input-source 1 external R010m
ptp clock ordinary domain 1
tod R0 ntp
input 1pps R0
clock-port master master
transport ipv4 unicast interface loopback 0

ToD/1PPS Configuration—Slave

ptp clock ordinary domain 1
tod R0 ntp
output 1pps R0 offset 200 pulse-width 20 μsec
clock-port SLA slave
transport ipv4 unicast interface loopback 0 negotiation
clock source 33.1.1.

Show Commands

Router# show ptp clock dataset ?
current currentDS dataset
default defaultDS dataset
parent parentDS dataset
time-properties timePropertiesDS dataset
Router# show ptp port dataset ?
foreign-master foreignMasterDS dataset
port portDS dataset
Router# show ptp clock running domain 0

<table>
<thead>
<tr>
<th>PTP Ordinary Clock [Domain 0]</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>ACQUIRING</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PTP Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>SLAVE</td>
</tr>
</tbody>
</table>

SESSION INFORMATION
SLAVE [Lo0] [Sessions 1]

<table>
<thead>
<tr>
<th>Peer addr</th>
<th>Pkts in</th>
<th>Pkts out</th>
<th>In Errs</th>
<th>Out Errs</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8.8.8</td>
<td>296399</td>
<td>98405</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Router# show platform software ptpd stat stream 0
LOCK STATUS : PHASE LOCKED
SYNC Packet Stats
- Time elapsed since last packet: 0.0
- Configured Interval: 0, Acting Interval: 0
- Tx packets: 0, Rx Packets: 169681
- Last Seq Number: 0, Error Packets: 1272
Delay Req Packet Stats
- Time elapsed since last packet: 0.0
- Configured Interval: 0, Acting Interval: 0
- Tx packets: 84595, Rx Packets: 0
- Last Seq Number: 19059, Error Packets: 0

Current Data Set
- Offset from master: 0.4230440
- Mean Path Delay: 0.0
- Steps Removed: 1

General Stats about this stream
- Packet rate: 0, Packet Delta (ns): 0
- Clock Stream handle: 0, Index: 0
- Oper State: 6, Sub oper State: 7
- Log mean sync Interval: -5, log mean delay req int: -4

Router# show platform ptp all
Slave info : [Loopback0][0x38A4766C]

--------------------------------
clock role : SLAVE
Slave Port hdl : 486539266
Tx Mode : Unicast-Negotiation
Slave IP : 4.4.4.4
Max Clk Srcs : 1
Boundary Clock : FALSE
Lock status : HOLDOVER
Refcnt : 1
Config-Flags : 0x7F - Clock Port Stream
Config-Ready-Flags : Port Stream
PTP Engine Handle : 0
Master IP : 8.8.8.8
Local Priority : 0
Set Master IP : 8.8.8.8

Router# show platform ptp tod all
--------------------------------
ToD/1PPS CONFIGURED : YES
ToD FORMAT : NMEA
ToD DELAY : 0
1PPS MODE : OUTPUT
OFFSET : 0
PULSE WIDTH : 0
ToD CLOCK : Mon Jan 1 00:00:00 UTC 1900

Router# show ptp clock running domain 0
PTP Boundary Clock [Domain 0]

State Ports Pkts sent Pkts rcvd Redundancy Mode
PHASE_ALIGNED 2 32355 159516 Hot standby

PORT SUMMARY

PTP Master
Name Tx Mode Role Transport State Sessions Port Addr
### Input Synchronous Ethernet Clocking

The following example shows how to configure the chassis to use the BITS interface and two Gigabit Ethernet interfaces as input synchronous Ethernet timing sources. The configuration enables SSM on the BITS port.

```
! Interface GigabitEthernet0/0
  synchronous mode
  network-clock wait-to-restore 720
!
Interface GigabitEthernet0/1
  synchronous mode
!
  network-clock synchronization automatic
  network-clock input-source 1 External R0 e1 crc4
  network-clock input-source 1 gigabitethernet 0/0
  network-clock input-source 2 gigabitethernet 0/1
  network-clock synchronization mode QL-enabled
  no network-clock revertive
```
CHAPTER 4

Using the Management Ethernet Interface

This chapter covers the following topics:

• Gigabit Ethernet Management Interface Overview, on page 87
• Gigabit Ethernet Port Numbering, on page 87
• IP Address Handling in ROMmon and the Management Ethernet Port, on page 88
• Gigabit Ethernet Management Interface VRF, on page 88
• Common Ethernet Management Tasks, on page 89

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 88.

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.
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:
    G10
  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
```

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, on page 93
- Verifying the Interface Configuration, on page 102
- Verifying Interface Module Status, on page 103
- Configuring LAN/WAN-PHY Controllers, on page 104
- Configuration Examples, on page 109

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

- Interface module A900-IMA8Z in slot 0 with A900-RSP3C-200-S supports a maximum of 6 ports at 10GE speed and needs explicit enablement using the `hw-module subslot 0/0 A900-IMA8Z mode 6-port` command.

- VRF-Aware Software Infrastructure (VASI) interface commands `interface vasilft` 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.

- 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.
• Mixed configurations of features are not supported on the same port. For example, one OC-3 port can have only CEM (CESoP or SAToP), ATM, IMA or DS3 configurations, but not a combination of these features on a single port.

• 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

### Configuring an Interface

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

**SUMMARY STEPS**

1. configure terminal
2. Do one of the following:
   • interface gigabitethernet slot/subslot/port
   • interface tengigabitethernet slot/subslot/port
3. ip address ip-address mask \{secondary\} | dhcp \{client-id interface-name\} \{hostname host-name\}
4. no negotiation auto
5. `speed { 10 | 100 | 1000 }`
6. `mtu bytes`
7. `standby [group-number] ip [ip-address [secondary]]`
8. `no shutdown`

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
| Step 2 | Do one of the following:  
- `interface gigabitethernet slot/subslot/port`
- `interface tengigabitethernet slot/subslot/port` | Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where: |
| Example: | `interface gigabitethernet 0/0/1` | Note: The slot number is always 0. |
| Example: | `interface tengigabitethernet 0/0/1` | |
| Step 3 | `ip address ip-address mask {secondary} | dhcp {client-id interface-name} [hostname host-name]` | Sets a primary or secondary IP address for an interface that is using IPv4, where: |
| Example: | `ip address 192.168.1.1 255.255.255.255 dhcp hostname host1` | |
| Step 4 | `no negotiation auto` | (Optional) Disables automatic negotiation. |
| Example: | `no negotiation auto` | Note: Use the `speed` command only when the mode is set to no negotiation auto. |
**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.

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>speed { 10</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# speed 1000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>mtu bytes</td>
<td>(As Required) Specifies the maximum packet size for an interface, where:</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# mtu 1500</td>
<td>- bytes—The maximum number of bytes for a packet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 1500 bytes; the range is from 1500 to 9216.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>standby [group-number] ip [ip-address [secondary]]</td>
<td>Creates or enables the Hot Standby Router Protocol (HSRP) group using its number and virtual IP address, where:</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# standby 250 ip 192.168.10.1</td>
<td>- (Optional) <strong>group-number</strong>—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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional on all but one interface if configuring HSRP) <strong>ip-address</strong>—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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) <strong>secondary</strong>—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 IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This command is required only for configurations that use HSRP.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This command enables HSRP but does not configure it further.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>no shutdown</td>
<td>Enables the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

---

**Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE Fuji 16.9.x**
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:

```bash
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:

```bash
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.
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
Hello time 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

**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 maximum configurable MTU is 9216 bytes. The interface module automatically adds an additional 22 bytes to the configured MTU size to accommodate some of the additional overhead.
Interface MTU Configuration Guidelines

When configuring the interface MTU size, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following additional overhead:
  - Layer 2 header—14 bytes
  - Dot1q header—4 bytes
  - CRC—4 bytes

- Interface MTU is not supported on BDI Interface

Configuring Interface MTU

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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. |

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>negotiation auto</td>
<td>Enables autonegotiation on a Gigabit Ethernet interface. Advertisement of flow control occurs.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no negotiation auto</td>
<td>Disables autonegotiation on Gigabit Ethernet interfaces. No advertisement of flow control occurs.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>Writes the new configuration to NVRAM.</td>
</tr>
</tbody>
</table>

For information about managing your system image and configuration files, refer to the Cisco IOS Configuration Fundamentals Configuration Guide and Cisco IOS Configuration Fundamentals Command Reference 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.
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 NCS4200-1TE1LR-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
```
Verifying Interface Module Status

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

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`.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `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 (1273)
  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 different 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
Configuring LAN-PHY Mode

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

SUMMARY STEPS

1. show controllers wanphy slot/subslot/port
2. configure terminal
3. Do the following:
   • hw-module subslot slot/subslot interface port enable LAN
4. exit
5. show controllers wanphy slot/subslot/port

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show controllers wanphy slot/subslot/port</td>
<td>Displays the configuration mode of the LAN/WAN-PHY controller. Default configuration mode is LAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show controllers wanphy 0/1/0</td>
<td></td>
</tr>
<tr>
<td>TenGigabitEthernet0/1/0</td>
<td>Mode of Operation: WAN Mode</td>
<td></td>
</tr>
<tr>
<td>SECTION</td>
<td>LOF = 0 LOS = 0</td>
<td></td>
</tr>
<tr>
<td>LINE</td>
<td>BIP(B1) = 0</td>
<td></td>
</tr>
<tr>
<td>AIS = 0 RDI = 0 FEBE = 0</td>
<td>BIP(B2) = 0</td>
<td></td>
</tr>
<tr>
<td>PATH</td>
<td>BIP(B3) = 0</td>
<td></td>
</tr>
<tr>
<td>AIS = 0 RDI = 0 FEBE = 0</td>
<td>BIP(B3) = 0</td>
<td></td>
</tr>
<tr>
<td>LOP = 0 NEWPTR = 0 PSE = 0</td>
<td>NSE = 0</td>
<td></td>
</tr>
<tr>
<td>WIS ALARMS</td>
<td>SER = 0 FELCDP = 0 FEAISP = 0</td>
<td></td>
</tr>
<tr>
<td>WLOD = 0 PLCD = 0</td>
<td>LFEBIP = 0 PBEC = 0</td>
<td></td>
</tr>
<tr>
<td>Active Alarms[All defects]: SWLOF LAIS PAIS SER</td>
<td>Active Alarms[Highest Alarms]: SWLOF</td>
<td></td>
</tr>
<tr>
<td>Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA</td>
<td>PLOP WLOS</td>
<td></td>
</tr>
<tr>
<td>Rx(K1/K2): 00/00 Tx(K1/K2): 00/00</td>
<td>S1S0 = 00, C2 = Ox1A</td>
<td></td>
</tr>
<tr>
<td>PATH TRACE BUFFER: UNSTABLE</td>
<td>Remote J1 Byte:</td>
<td></td>
</tr>
<tr>
<td>BER thresholds: SD = 10e-6 SF = 10e-3</td>
<td>TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

Do the following:

- `hw-module subslot slot/subslot interface port enable LAN`

Example:

Router(config)# hw-module subslot 0/1 enable LAN

Example:

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

**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

**Configuring WAN-PHY Mode**

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

**SUMMARY STEPS**

1. `show controllers wanphy slot/subslot/port`
2. `configure terminal`
3. Do the following:
   - `hw-module subslot slot/subslot interface port enable WAN`
4. `exit`
5. `show controllers wanphy slot/subslot/port`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show controllers wanphy slot/subslot/port</td>
<td>Displays the configuration mode of the WAN-PHY controller. Default configuration mode is LAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>slot/subslot/port</em>—The location of the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# show controllers wanphy 0/1/0</td>
</tr>
<tr>
<td></td>
<td>TenGigabitEthernet0/1/0</td>
</tr>
<tr>
<td></td>
<td><strong>Mode of Operation: LAN Mode</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> Do the following:</td>
<td>Configures WAN-PHY mode for the Ethernet interface module.</td>
</tr>
<tr>
<td><strong>• hw-module subslot slot/subslot interface port enable WAN</strong></td>
<td><em>slot/subslot</em>—The location of the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Use the <strong>hw-module subslot slot/subslot interface port enable WAN</strong> command to configure the WAN-PHY mode for the Ethernet interface module.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# hw-module subslot 0/1 enable WAN</td>
</tr>
<tr>
<td></td>
<td>Router(config)# hw-module subslot 0/1 interface 1 enable WAN</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits global configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# exit</td>
</tr>
<tr>
<td><strong>Step 5</strong> show controllers wanphy slot/subslot/port</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# show controllers wanphy 0/1/5</td>
</tr>
<tr>
<td></td>
<td>TenGigabitEthernet0/1/5</td>
</tr>
<tr>
<td></td>
<td><strong>Mode of Operation: WAN Mode</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SECTION</strong></td>
</tr>
<tr>
<td></td>
<td><strong>LOF</strong> = 0 <strong>LOS</strong> = 0 <strong>BIP(B1)</strong> = 0</td>
</tr>
<tr>
<td></td>
<td><strong>LINE</strong></td>
</tr>
<tr>
<td></td>
<td><strong>AIS</strong> = 0 <strong>RDI</strong> = 0 <strong>BIP(B2)</strong> = 0</td>
</tr>
<tr>
<td></td>
<td><strong>PATH</strong></td>
</tr>
<tr>
<td></td>
<td><strong>AIS</strong> = 0 <strong>RDI</strong> = 0 <strong>BIP(B3)</strong> = 0</td>
</tr>
<tr>
<td></td>
<td><strong>LOF</strong> = 0 <strong>NEWPTR</strong> = 0 <strong>PSE</strong> = 0</td>
</tr>
<tr>
<td></td>
<td><strong>NSE</strong> = 0</td>
</tr>
<tr>
<td></td>
<td><strong>WIS ALARMS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SER</strong> = 0 <strong>FELCDP</strong> = 0 <strong>FEAISP</strong> = 0</td>
</tr>
<tr>
<td></td>
<td><strong>0</strong></td>
</tr>
</tbody>
</table>
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.

SUMMARY STEPS

1. configure terminal
2. controller wanphy slot/subslot/port
3. wanphy {delay | flag | report-alarm | threshold {b1-tca | b2-tca | sd-ber | sf-ber [bit error rate]}}
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>controller wanphy slot/subslot/port</td>
<td>Enters WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN-PHY controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller wanphy 0/3/0</td>
<td><em>slot/subslot/port</em> — The location of the interface.</td>
</tr>
</tbody>
</table>
## 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.

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

! Configure an IP address.
```
Example: MTU Configuration

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.

![Image 101x350 to 118x366]

![Image 101x255 to 118x271]
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.
!
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.
Example: VLAN Encapsulation
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 Cisco IOS Configuration Fundamentals Command Reference 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, on page 113
- Verifying the Interface Configuration, on page 130
- Configuration Examples, on page 131

Configuration Tasks

This section describes how to configure the T1/E1 interface module for the chassis and 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-port T1/E1 interface module
  - 32-port T1/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:

#### SUMMARY STEPS

1. **configure terminal**
2. **card type {e1 | t1} slot/subslot**
3. **exit**

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

  **configure terminal**

Example:

```
Router# configure terminal
```

| **Step 2**

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

Example:

```
Router(config)# card type e1 0/3
```
### Enabling T1 Controller

**Note**

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

To enable T1 controller:

```plaintext
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:

**SUMMARY STEPS**

1. `configure terminal`
2. `controller {t1 | e1} slot/subslot/port`
3. `clock source {internal | line}`
4. `linecode {ami | b8zs | hdb3}`
5. For T1 Controllers:
6. `cablelength {long | short}`
7. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>
### Configuring the Controller

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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:
framing \{sf | esf\}  
Example:
Router(config-controller)# framing sf | 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. |
| For E1 Controllers:  
framing \{crc4 | no-crc4\}  
Example:
Router(config-controller)# framing crc4 | — |
### Configuring T1/E1 Interfaces

#### 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
  Cable length 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.

**SUMMARY STEPS**

1. `configure terminal`
2. `controller {t1 | e1} slot/subslot/port`
3. For T1 controllers
4. `exit`
## Detailed Steps

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>controller {t1</td>
<td>e1} slot/subslot/port</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# controller t1 0/3/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t1—Specifies the T1 controller.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• e1—Specifies the E1 controller.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• slot/subslot/port—Specifies the location of the controller.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The slot number is always 0.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For T1 controllers</td>
<td>Sets the framing on the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>framing {sf</td>
<td>esf}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# framing sf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• sf—Specifies Super Frame as the T1 frame type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• esf—Specifies Extended Super Frame as the T1 frame type. This is the default for T1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For E1 controllers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>framing {crc4</td>
<td>no-crc4}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# framing crc4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• crc4—Specifies CRC4 frame as the E1 frame type. This is the default for E1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• no-crc4—Specifies no CRC4 as the E1 frame type.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

## Verifying Framing Configuration

Use the show controllers command to verify the framing configuration:

```bash
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
```
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.

SUMMARY STEPS

1. interface serial 0/subslot/port:channel-group
2. ip address address mask
3. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> interface serial 0/subslot/port:channel-group</td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface serial 0/0/1:0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ip address address mask</td>
<td>Sets the IP address and subnet mask.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 192.0.2.1 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>
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:

**SUMMARY STEPS**

1. configure terminal
2. interface serial 0/subslot/port:channel-group
3. encapsulation {hdlc | ppp}
4. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface serial 0/subslot/port:channel-group</td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# interface serial 0/0/1:0</td>
<td></td>
</tr>
<tr>
<td>Step 3 encapsulation {hdlc</td>
<td>ppp}</td>
</tr>
<tr>
<td>Example: Router(config-if)# encapsulation hdlc</td>
<td></td>
</tr>
</tbody>
</table>
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 runs, 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:
### SUMMARY STEPS

1. `configure terminal`
2. `interface serial 0/subslot/port:channel-group`
3. `crc {16 | 32}`
4. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**        | Selects the interface to configure from global configuration mode. |
| interface serial 0/subslot/port:channel-group |         |
| Example:          |         |
| Router(config)# interface serial 0/0/1:0 |         |
| Example:          |         |

- `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**        | Selects the CRC size in bits. |
| crc {16 | 32} |         |
| Example:          |         |
| Router(config-if)# crc 16 |         |
| **Note**          | Moving from CRC 16 to 32 bit (and vice-versa) is not supported. |

| **Step 4**        | Exits configuration mode and returns to the EXEC command interpreter prompt. |
| exit              |         |
| Example:          |         |
| Router(config)# exit |         |

### 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:

**SUMMARY STEPS**

1. `configure terminal`
2. `controller {t1 | e1} slot/subslot/port`
3. `channel-group [t1 | e1] number {timeslots range | unframed} [speed {56 | 64}]`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **configure terminal**<br>**Example:**

Router# `configure terminal`

| **Step 2** | **controller {t1 | e1} slot/subslot/port**<br>**Example:**

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

| **Step 3** | **channel-group [t1 | e1] number {timeslots range | unframed} [speed {56 | 64}]**<br>**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.
### Saving the Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>Writes the new configuration to NVRAM.</td>
</tr>
</tbody>
</table>

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 124
- Running Bit Error Rate Testing, on page 126

### 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:

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

Setting a Loopback on the T1 Controller

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller t1 slot/subslot/port</td>
<td>Selects the T1 controller and enter controller configuration mode. The slot number is always 0.</td>
<td></td>
</tr>
<tr>
<td>loopback diag</td>
<td></td>
<td>Sets a diagnostic loopback on the T1 line.</td>
</tr>
<tr>
<td>loopback local {line</td>
<td>payload}</td>
<td>Sets a local loopback on the T1 line. You can select to loopback the line or the payload.</td>
</tr>
<tr>
<td>loopback remote iboc</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>end</td>
<td></td>
<td>Exits configuration mode when you have finished configuring the controller.</td>
</tr>
</tbody>
</table>

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

Table 13: Loopback Descriptions

<table>
<thead>
<tr>
<th>Loopback</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loopback diag</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Loopback**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>loopback local</strong></td>
</tr>
<tr>
<td><strong>local line</strong></td>
</tr>
<tr>
<td><strong>local payload</strong></td>
</tr>
<tr>
<td><strong>loopback remote iboc</strong></td>
</tr>
<tr>
<td><strong>network line</strong></td>
</tr>
<tr>
<td><strong>network payload</strong></td>
</tr>
</tbody>
</table>

---

**Running 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

**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 14: BERT Pattern Descriptions

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0s</td>
<td>Repeating pattern of zeros (...000...).</td>
</tr>
<tr>
<td>1s</td>
<td>Repeating pattern of ones (...111...).</td>
</tr>
<tr>
<td>2^11</td>
<td>Pseudo-random test pattern that is 2,048 bits in length.</td>
</tr>
<tr>
<td>2^15</td>
<td>Pseudo-random O.151 test pattern that is 32,768 bits in length.</td>
</tr>
<tr>
<td>2^20-O153</td>
<td>Pseudo-random O.153 test pattern that is 1,048,575 bits in length.</td>
</tr>
<tr>
<td>2^20-QRSS</td>
<td>Pseudo-random QRSS O.151 test pattern that is 1,048,575 bits in length.</td>
</tr>
<tr>
<td>2^23</td>
<td>Pseudo-random 0.151 test pattern that is 8,388,607 bits in length.</td>
</tr>
<tr>
<td>alt-0-1</td>
<td>Repeating alternating pattern of zeros and ones (...01010...).</td>
</tr>
</tbody>
</table>

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.
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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show controllers {e1</td>
<td>t1} [slot/port-adapter/port/e1-line] [brief]`</td>
</tr>
<tr>
<td><code>show interface serial slot/subslot/port</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>clear counters serial slot/subslot/port</code></td>
<td>Clears the interface counters</td>
</tr>
</tbody>
</table>

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 pseudowire went down. Now, AIS alarm are generated when the pseudowire 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.
- Pseudowire 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
core controller E1 0/3/0
ais-core-failure
framing unframed
```
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: 1111
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 (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
    18087311 packets input, 61438015508 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
```
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:

```bash
! 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:

```bash
! 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
```
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

Configuring Serial Interfaces

This chapter configures the serial interface module (PN: A900-IMASER14A/S) Async/Sync R232 serial data using Transparent Pseudowire (PW) over MPLS network and raw socket. 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 Cisco IOS Configuration Fundamentals Command Reference 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.

• Information About Serial Interface Module, on page 133
• Restrictions, on page 134
• How to Configure Serial Interface, on page 135
• Verifying the Serial Interface Configuration, on page 144
• Configuration Examples, on page 146

Information About Serial Interface Module

The serial interface module supports pseudowire transport over MPLS and raw socket for Async and Sync traffic. The Serial IM interfaces monitor and detect cable connections, cable types and also monitors modem control signals periodically.
The A900-IMASER14A/S interface provides a direct connection between the Cisco router and external networks.

**Note**

We recommend that you use a smart serial or 4-port octopus cable to connect the A900-IMASER14A/S with the external network.

Out of 14 ports, 6 ports support sync interfaces and 8 ports support async interfaces. RS232 Async data is carried over Raw Socket and Transparent byte mode and RS232 Sync data is carried over Raw Socket.

**Restrictions**

This section describes the port restrictions for Serial interface module:

- Ports 0-7 are Async ports on the 68-pin connector
- Ports 8-13 are Sync or Async on the 12-in-1 connector

**Note**

Sync is not supported in Cisco IOS XE Release 3.14S. Sync ports cannot be configured in Cisco IOS XE Release 3.14S.

- Maximum speed on all ports is 236Kbps.

This section describes the software limitations that apply when configuring the Serial interface module:
• The router can only be configured as data circuit-terminating equipment (DCE).
• Configuration of pseudowire between local and remote PE with different speed on Sync and Async ports is not supported.
• Sub-rate (below DS0 bandwidth) Async (R232) data over MPLS using T1/E1 CESoP is not supported.
• Pseudowire ping is not supported for the pseudowire configured on the serial interface module.
• Only two serial interface modules can come up on the router in release prior to Cisco IOS XE Release 3.14. Starting with Cisco IOS XE Release 3.14, all 6 bays on the router are available for insertion of interface modules simultaneously.
• Only Trans encapsulation is supported in Cisco IOS XE Release 3.14S.
• If you installed a new A900-IMASER14A/S or if you want to change the configuration of an existing interface, you must enter configuration mode to configure the new interfaces. If you replaced an A900-IMASER14A/S that was previously configured, the system recognizes the new interfaces and brings each of them up in their existing configuration.
• Pseudowire ping is not supported for cross-connect configured on A900-IMA14A/S interface module.
• A maximum speed of 64 kbps between PE and DTE is supported for RS232 Sync ports.
• PE can act only as DCE and provides the clock to DTE.
• Serial IM Sync signaling transport does not interoperate with the third party equipments. HLDC frames used for transport of these signals are Cisco-specific.

How to Configure Serial Interface

Required Configuration Tasks

Configuring the Controller

To create the interfaces for the Serial interface module, complete these steps:

SUMMARY STEPS

1. configure terminal
2. controller serial slot/subslot/port
3. physical-layer async | sync
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Router# configure terminal**

<table>
<thead>
<tr>
<th>Step 2</th>
<th>controller serial slot/subslot/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller serial 0/4/1</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

Selects the controller to configure and enters controller configuration mode.

- **slot/subslot/port** — Specifies the location of the interface.

**Note**

The slot number is always 0.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>physical-layer async</th>
<th>sync</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# physical-layer async</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

Configures the serial interface in async or sync mode.

- async — Specifies async interface.
- sync — Specifies sync interface. This is the default mode.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

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

### Example: Controller Configuration

```plaintext
Router# configure terminal
Router(config)# controller 0/4/1
Router(config-controller)# physical-layer async
Router(config)# exit
```

### Optional Configurations

#### Configuring Layer 1 on Sync and Async Interface Server

The RS232 which is enabled by default on the async interface, supports RS232 DCE cable with the DB-25 connector. The Cisco smart serial cable with the DB-25 connector supports RS232 and RS485. The RJ45 cable type supports only RS485.

#### SUMMARY STEPS

1. configure terminal
2. line slot/bay/port
3. databits \{5 | 6 | 7 | 8\}
4. stopbits \{1 | 1.5 | 2\}
5. speed speed-value
6. raw-socket tcp server port server ip address
7. raw-socket packet length packet length
8. flowcontrol \{none | software \{lock | in | out\} | hardware \{in | out\} \}
9. **parity** \{**even** | **mark** | **none** | **odd** | **space**\}
10. **sig-transport u-frame pattern** \(pattern\)
11. **control-sig-transport** \[**on** | **off**\]
12. **connection-topology** \[**point-to-point** | **point-to-multipoint**\]
13. **exit**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Selects the controller to configure and enters serial interface configuration mode.</td>
</tr>
<tr>
<td><code>line slot/bay/port</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# line 0/4/1</code></td>
<td>Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the databit configuration. The default is 8.</td>
</tr>
<tr>
<td>`databits {5</td>
<td>6</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-line)# databits 8</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets the stopbit configuration. The default is 2.</td>
</tr>
<tr>
<td>`stopbits {1</td>
<td>1.5</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-line)# stopbits 2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies the serial interface speed. The valid range is from 300 to 230400. The default is 9600.</td>
</tr>
<tr>
<td><code>speed speed-value</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-line)# speed 9600</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies raw-tcp server configuration.</td>
</tr>
<tr>
<td><code>raw-socket tcp server port server ip address</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-line)# raw-socket tcp server 5000 1.1.1.1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Specifies raw-tcp packet length configuration options.</td>
</tr>
<tr>
<td><code>raw-socket packet length packet length</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-line)# raw-socket packet-length 32</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Sets the flowcontrol.</td>
</tr>
<tr>
<td>`flowcontrol /none</td>
<td>software [lock</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# flowcontrol none</td>
<td>• none</td>
</tr>
<tr>
<td></td>
<td>• software</td>
</tr>
<tr>
<td></td>
<td>• hardware</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Sets the parity.</td>
</tr>
<tr>
<td>parity {even</td>
<td>mark</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# parity none</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>This step is specific to Sync mode only. Specifies the u-frame format used for internal signal transport.</td>
</tr>
<tr>
<td>sig-transport u-frame pattern</td>
<td>pattern</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# sig-transport u-frame pattern NR0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>This step is specific to Sync mode only. Specifies if the hardware control signals need to be sent to the remote PE.</td>
</tr>
<tr>
<td>control-sig-transport [on</td>
<td>off]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# control-sig-transport on</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>This step is specific to Sync mode only. Specifies the type of topology.</td>
</tr>
<tr>
<td>connection-topology [point-to-point</td>
<td>point-to-multipoint]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# connection-topology point-to-multipoint</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Async Layer 1 Parameters**

```
Router# configure terminal
Router(config)# line 0/4/1
Router(config-line)# databits 8
Router(config-line)# stopbits 2
Router(config-line)# speed 9600
Router(config-line)# flow-control none
Router(config-line)# parity none
Router(config-line)# exit
```

**Configuring Layer 1 on Sync and Async Interface Client**

**SUMMARY STEPS**

1. configure terminal
2. line slot/bay/port
3. databits {5 | 6 | 7 | 8}
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>line slot/bay/port</code></td>
<td>Select the controller to configure and enters serial interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>- <em>slot/subslot/port</em>—Specifies the location of the interface.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# <code>line 0/4/1</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`databits {5</td>
<td>6</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-line)# <code>databits 8</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>`stopbits {1</td>
<td>1.5</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-line)# <code>stopbits 2</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>speed speed-value</code></td>
<td>Specifies the serial interface speed. The valid range is form 300 to 230400. The default is 9600.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-line)# <code>speed 9600</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>raw-socket tcp client server ip address server port client ip address client port</code></td>
<td>Specifies raw-tcp client configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-line)# <code>raw-socket tcp client 1.1.1.1 5000 10.10.10.10 9000</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>raw-socket packet length packet length</code></td>
<td>Specifies raw-tcp packet length configuration options.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-line)# <code>raw-socket packet-length 32</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Channel Group

**SUMMARY STEPS**

1. configure terminal
2. controller serial *slot/bay/port*
3. channel-group *channel-group*
4. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> controller serial <em>slot/bay/port</em></td>
<td>Configures the controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller serial 0/4/1</td>
<td><em>slot/subslot/port</em>—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> channel-group <em>channel-group</em></td>
<td>Configures the channel group with specified NxDS0 time slots.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# channel-group 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Serial Interfaces

Example: Channel Group

```
Router# configure terminal
Router(config)# controller serial 0/4/1
Router(config-controller)# channel-group 0
Router(config-controller)# exit
```

Configuring Encapsulation

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

SUMMARY STEPS

1. configure terminal
2. interface serial slot/bay/port
3. encapsulation {ppp|raw-tcp | trans | sdmc}
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface serial slot/bay/port</td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# interface serial 0/4/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> encapsulation {ppp</td>
<td>raw-tcp</td>
</tr>
<tr>
<td>Example: Router(config-if)# encapsulation raw-tcp</td>
<td></td>
</tr>
</tbody>
</table>

- **ppp**—Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.
- **trans**—Transparent encapsulation.

**Note**Trans encapsulation is supported on the access side for serial interfaces which has cross connect configured.

- **sdmc**—Switched Multimegabit Data Services (SDMC) for serial interface.
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>

### Purpose

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

---

### Configuring Transparent Pseudowire (PW) Cross-Connect

Transparent PW mode provides a facility to configure the speed between 300 bps to 230400 bps.

### SUMMARY STEPS

1. configure terminal
2. interface serial slot/bay/port
3. xconnect peer-router-id vcid encapsulation mpls
4. exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal Example: Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface serial slot/bay/port Example: Router(config)# interface serial 0/4/1</td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• slot/subslot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> xconnect peer-router-id vcid encapsulation mpls Example: Router(config-if)# xconnect 1.1.1.1 1001 encapsulation mpls</td>
<td>Configures the VC to transport packets.</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit Example: Router(config)# exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
</tbody>
</table>

---

Example: Transparent Pseudowire on Cross Connect

```bash
Router# configure terminal
Router(config)# interface serial 0/4/1
```
Configuring Invert Clock Signal

SUMMARY STEPS

1. configure terminal
2. controller serial slot/bay/port
3. invert data
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>controller serial slot/bay/port</td>
<td>Configures the controller.</td>
</tr>
<tr>
<td>Example:</td>
<td>slot/subslot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# controller serial 0/4/1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>invert data</td>
<td>Configures the invert data clock signal.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# invert data</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits configuration mode and returns to the EXEC</td>
</tr>
<tr>
<td>Example:</td>
<td>command interpreter prompt.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>

Example: Invert Data on the Serial Interface

The following example shows invert data configuration on the serial interface.

```
Router# configure terminal
Router(config)# controller serial 0/4/1
Router(config-controller)# invert data
Router(config-controller)# exit
```

Configuring NRZI Formats

SUMMARY STEPS

1. configure terminal
2. \texttt{interfaceserial} \textit{slot/bay/port}

3. \texttt{nrzi-encoding}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example:
  
  Router# \texttt{configure terminal} |

| **Step 2** interfaceserial \textit{slot/bay/port} | Select the controller to configure and enters serial interface configuration mode. |
| Example:
  
  Router(config)# interface serial 0/4/1 | \textit{slot/subslot/port}—Specifies the location of the interface. |

| **Step 3** nrzi-encoding | Enable NRZI encoding. |
| Example:
  
  Router(config-if)# nrzi-encoding | To disable NRZI encoding, use the no form of the command. |

**Saving the Configuration**

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{copy running-config startup-config}</td>
<td>Writes the new configuration to NVRAM.</td>
</tr>
</tbody>
</table>

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.

**Verifying the Serial Interface Configuration**

Use the following commands to verify the configuration the serial interface

- \texttt{show controllers serial \textit{slot/bay/port}}

Use the \texttt{show controllers serial \textit{slot/bay/port}} command to display serial interface configuration on the router.

```plaintext
Router# show controllers serial 0/1/0
Serial0/1/0 - (A900-IMASER14A/S) is up
  Encapsulation : RAW-TCP
  Cable type: RS-232 DCE
  mtu 1500, max_buffer_size 1524, max_pak_size 1524 enc 84
  loopback: Off, crc: 16, invert_data: Off
  nrzi: Off, idle char: Flag
dce_terminal_timing_enable: Off ignore_dtr: Off
  serial_clockrate: 64000bps, serial_clock_index: 14 serial_restartdelay:30000,
```
serial_restartdelay_def:30000

DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

• show interfaces serial slot/bay/port

Use the show interfaces serial slot/bay/port command to display serial interface packet status information, model control signal status information on the router.

Router# show interfaces serial 0/1/0
Serial0/1/0 is up, line protocol is up
Hardware is A900-IMASER14A/S
MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec, reliability 255/255, txload 47/255, rxload 103/255
Encapsulation RAW-TCP, loopback not set
Keepalive not supported
Last input never, output 00:00:00, output hang never
Last clearing of "show interface" counters 00:38:06
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 26000 bits/sec, 69 packets/sec
5 minute output rate 12000 bits/sec, 69 packets/sec
157782 packets input, 7562229 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 abort
156862 packets output, 346071 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

• show running-config interface serial slot/bay/port

Use the show running-config interface serial slot/bay/port command to display serial interface IP address information, keep alive and cross-connect status information on the router.

Router# show running-config interface serial 0/1/0
Building configuration...
Current configuration : 107 bytes
!
interface Serial0/1/0
no ip address
encapsulation trans
xconnect 1.1.1.1 1001 encapsulation mpls
End

• show xconnect all

Use the show xconnect all to command to display all cross connect status on the router.

Router# show xconnect all
Legend: XC ST=Xconnect State S1=Segment1 State S2=Segment2 State
UP=Up  DM=Down  AD=Admin Down  IA=Inactive
SB=Standby HS=Hot Standby RV=Recovering NH=No Hardware
XC ST  Segment 1  S1  Segment 2  S2  -----------------------------
UF pri  ac Se0/1/0(HDLC)  UF mpls 1.1.1.1:1001  UP
Use the `show raw-socket tcp sessions` and `show raw-socket tcp statistic` commands to display the raw socket status.

```
Router#show raw-socket tcp sessions
-------------------------------------------------- TCP Sessions
------------------------------------------------------
<table>
<thead>
<tr>
<th>Interface tty</th>
<th>vrf_name</th>
<th>socket_mode</th>
<th>local_ip_addr</th>
<th>local_port</th>
<th>dest_ip_addr</th>
<th>dest_port</th>
<th>up_time</th>
<th>idle_time/timeout</th>
<th>local_ip_addr</th>
<th>local_port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/3/12</td>
<td>154</td>
<td>server</td>
<td>20.20.20.20</td>
<td>5000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>listening</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/3/12</td>
<td>154</td>
<td>server</td>
<td>20.20.20.20</td>
<td>5000</td>
<td>10.10.10.10</td>
<td>9000</td>
<td>00:20:49</td>
<td>00:00:00/5 min</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

```
Router#show raw-socket tcp statistic
-------------------------------------------- TCP-Serial Statistics
-----------------------------------------
<table>
<thead>
<tr>
<th>Interface tty</th>
<th>vrf_name</th>
<th>sessions</th>
<th>tcp_in_bytes</th>
<th>tcp_out_bytes</th>
<th>tcp_to_tty_frames</th>
<th>tty_to_tcp_frames</th>
<th>tcp_in_bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/3/12</td>
<td>154</td>
<td>1</td>
<td>1847204</td>
<td>4640310</td>
<td>87709</td>
<td>87671</td>
<td>1847204</td>
</tr>
</tbody>
</table>
```

**Configuration Examples**

This section includes the following configuration examples:

**Example: Encapsulation Configuration**

The following example sets encapsulation for the controller and interface:

**PE1 CONFIG**

```
controller SERIAL 0/1/0
physical-layer async
channel-group 0
interface Serial0/1/0
no ip address
encapsulation tran
xconnect 2.2.2.2 1001 encapsulation mpls
```

**PE2 CONFIG**

```
controller SERIAL 0/2/0
physical-layer async
channel-group 0
interface Serial0/2/0
no ip address
encapsulation tran
xconnect 1.1.1.1 1001 encapsulation mpls
```
CHAPTER 8

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, on page 147
- Restrictions for Dying Gasp Support, on page 147
- Configuration Examples for Dying Gasp Support, on page 148
- Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations, on page 148
- Message Displayed on the Peer Router on Receiving Dying Gasp Notification, on page 150
- Displaying SNMP Configuration for Receiving Dying Gasp Notification, on page 150
- Dying GASP via SNMP Trap Support on Cisco RSP3 Module, on page 150

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

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)#
Router(config)# ^Z
Router#

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

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

---

Note

---

This is not supported on Cisco RSP1 and Cisco RSP2 modules.
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 notification, 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
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:

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

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

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

### Verifying SNMP Host Configuration

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

```plaintext
#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
```
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 9

Configuring the Global Navigation Satellite System

The chassis uses a satellite receiver, also called the global navigation satellite system (GNSS), as a new timing interface.

In typical telecom networks, synchronization works in a hierarchal manner where the core network is connected to a stratum-1 clock and this clock is then distributed along the network in a tree-like structure. However, with a GNSS receiver, clocking is changed to a flat architecture where access networks can directly take clock from satellites in sky using an on-board GPS chips.

This capability simplifies network synchronization planning, provides flexibility and resilience in resolving network synchronization issues in the hierarchical network.

- Information About the GNSS, on page 153
- How to Configure the GNSS, on page 155
- Configuration Example For Configuring GNSS, on page 158
- Additional References, on page 158

Information About the GNSS

Overview of the GNSS Module

The GNSS module is present on the front panel of the RSP3 module and can be ordered separately with PID=. However, there is no license required to enable the GNSS module.

The GNSS LED on the RSP3 front panel indicates the status of the module. The following table explains the different LED status.

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>GNSS Normal State. Self survey is complete.</td>
</tr>
<tr>
<td>Amber</td>
<td>All other states</td>
</tr>
</tbody>
</table>

When connected to an external antenna, the module can acquire satellite signals and track up to 32 GNSS satellites, and compute location, speed, heading, and time. GNSS provides an accurate one pulse-per-second
(PPS), a stable 10 MHz frequency output to synchronize broadband wireless, aggregation and pre-aggregation routers, and an accurate time-of-day (ToD).

**Note**

The RSP3 module can also receive 1PPS, 10 MHz, and ToD signals from an external clocking and timing source. However, the timing signals from the GNSS module (when enabled) take precedence over those of the external source.

By default, anti-jamming is enabled on the GNSS module.

### Operation of the GNSS Module

The GNSS module has the following stages of acquiring and providing timing signals to the Cisco router:

- **Self-Survey Mode**—When the router is reset, the GNSS module comes up in self-survey mode. It tries to lock on to minimum four different satellites and computes approximately 2000 different positions of the satellites to obtain a 3-D location (Latitude, Longitude, and Height) of it current position. This operation takes about 35-to-40 minutes. During this stage also, the module is able to generate accurate timing signals and achieve a *Normal* or *Phase-locked* state.

When GNSS moves into *Normal* state, you can start using the 1PPS, 10 MHz, and ToD inputs from GNSS. The quality of the signal in Self-Survey mode with *Normal* state is considered good enough to lock to GNSS.

- **Over determined clock mode**—The router switches to over determined (OD) mode when the self-survey mode is complete and the position information is stored in non-volatile memory on the router. In this mode, the module only processes the timing information based on satellite positions captured in self-survey mode.

The router saves the tracking data, which is retained even when the router is reloaded. If you want to change the tracking data, use the `no shutdown` command to set the GNSS interface to its default value.

The GNSS module stays in the OD mode unless one of the following conditions occur:

- A position relocation of the antenna of more than 100 meters is detected. This detection causes an automatic restart of the self-survey mode.

- A manual restart of the self-survey mode or when the stored reference position is deleted.

- A worst-case recovery option after a jamming-detection condition that cannot be resolved with other methods.

You can configure the GNSS module to automatically track any satellite or configure it to explicitly use a specific constellation. However, the module uses configured satellites only in the OD mode.

**Note**

GLONASS and BeiDou satellites cannot be enabled simultaneously. GALILEO is not supported.

When the router is reloaded, it always comes up in the OD mode unless:

- the router is reloaded when the Self-Survey mode is in progress

- the physical location of the router is changed to more than 100 m from it’s pre-reloaded condition.
When the GNSS self-survey is restarted using the default `gnss slot R0/R1` command in config mode, the 10MHz, 1PPS, and ToD signals are not changed and remain up.

**Anti-Jamming**

By default, anti-jamming is enabled on the GNSS module.

**High Availability for GNSS**

The chassis has two GNSS modules, one each on the active and standby RSP3 modules. Each GNSS module must have a separate connection to the antenna in case of an RSP3 switchover.

**Prerequisites for GNSS**

To use GNSS:

- 1PPS, 10 MHz, and ToD must be configured for netsync and PTP. For more information see the Configuring Clocking and Timing chapter.
- The antenna should see as much as possible from the total sky. For proper timing, minimum of four satellites should be locked. For information, see the *Cisco NCS 4206 Series Hardware Installation Guide*.

**Restrictions for GNSS**

The GNSS module is not supported through SNMP; all configurations are performed through commands.

**How to Configure the GNSS**

To know more about the commands referenced in this document, see the *Cisco IOS Master Command List*.

**Enabling the GNSS License**

```
enable
configure terminal
license feature gnss
exit
```

**Enabling the GNSS on the Cisco Router**

```
enable
configure terminal
gnss slot r0
no shutdown
exit
```
After the GNSS module is enabled, GNSS will be the source for 1PPS, ToD, and 10MHz clocking functions.

### Configuring the Satellite Constellation for GNSS

```
enable
cfg term
gnss slot r0
cstl [auto | gps | galelio | beidou | qzss]
exit
```

### Configuring Pulse Polarity

```
enable
cfg term
gnss slot r0
1pps polarity negative
exit
```

**Note** The `no 1pps polarity negative` command returns the GNSS to default mode (positive is the default value).

### Configuring Cable Delay

```
enable
cfg term
gnss slot r0
1pps offset 5
exit
```

**Note** It is recommended to compensate 5 nanosecond per meter of the cable.

The `no 1pps offset` command sets cable delay offset to zero.

### Disabling Anti-Jam Configuration

```
enable
cfg term
gnss slot
r0
anti-jam disable
exit
```
Verifying the Configuration of the GNSS

Use the `show gnss status` command to display status of GNSS.

```
Router# show gnss status
GNSS status:

  GNSS device: detected
  Lock status: Normal
  Receiver Status: Auto
  Clock Progress: Phase Locking
  Survey progress: 100
  Satellite count: 22
  Holdover Duration: 0
  PDOP: 1.04  TDOP: 1.00
  HDOP: 0.73  VDOP: 0.74
  Minor Alarm: NONE
  Major Alarm: None
```

Use the `show gnss satellite` command to display the status of all satellite vehicles that are tracked by the GNSS module.

```
Router# show gnss satellite all
All Satellites Info:

<table>
<thead>
<tr>
<th>SV PRN No</th>
<th>Channel No</th>
<th>Acq Flg</th>
<th>Ephemeris Flg</th>
<th>SV Type</th>
<th>Sig Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>47</td>
</tr>
<tr>
<td>21</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>47</td>
</tr>
<tr>
<td>22</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>46</td>
</tr>
<tr>
<td>18</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>46</td>
</tr>
<tr>
<td>27</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>47</td>
</tr>
<tr>
<td>31</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>49</td>
</tr>
<tr>
<td>24</td>
<td>10</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>42</td>
</tr>
<tr>
<td>79</td>
<td>12</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>78</td>
<td>13</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>26</td>
</tr>
</tbody>
</table>
```

```
Router# show gnss satellite 21
Selected Satellite Info:

  SV PRN No: 21
  Channel No: 2
  Acquisition Flag: 1
  Ephemeris Flag: 1
  SV Type: 0
  Signal Strength: 47
```

```
Router# show gnss time
Current GNSS Time:

  Time: 2015/10/14 12:31:01 UTC Offset: 17
```

```
Router# show gnss location
Current GNSS Location:

  LOC: 12:56.184000N 77:41.768000E 814.20 m
```

Use the `show gnss device` to displays the hardware information of the active GNSS module.
Router# show gnss device
GNSS device:
  Serial number: F0C2130ND5X
  Firmware version: 1.4
  Firmware update progress: NA
  Authentication: Passed

Configuration Example For Configuring GNSS

gnss slot R0
no shutdown
anti-jam disable
costellation glonass
1pps polarity negative
1pps offset 1000 negative

Additional References

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There are no associated standards for this feature,</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>•</td>
<td>There are no MIBs for this feature.</td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There are no associated RFCs for this feature.</td>
</tr>
</tbody>
</table>
G.8275.1 Telecom Profile

First Published: March 29, 2016

Precision Time Protocol (PTP) is a protocol for distributing precise time and frequency over packet networks. PTP is defined in the IEEE Standard 1588. It defines an exchange of timed messages.

PTP allows for separate profiles to be defined in order to adapt PTP for use in different scenarios. A profile is a specific selection of PTP configuration options that are selected to meet the requirements of a particular application.

This recommendation allows for proper network operation for phase and time synchronization distribution when network equipment embedding a telecom boundary clock (T-BC) and a telecom time slave clock (T-TSC) is timed from another T-BC or a telecom grandmaster clock (T-GM). This recommendation addresses only the distribution of phase and time synchronization with the full timing support architecture as defined in ITU-T G.8275.

- Why G.8275.1?, on page 159
- Configuring the G.8275.1 Profile, on page 163
- Additional References, on page 168
- Feature Information for G.8275.1, on page 168

Why G.8275.1?

The G.8275.1 profile is used in mobile cellular systems that require accurate synchronization of time and phase. For example, the fourth generation (4G) of mobile telecommunications technology.

The G.8275.1 profile is also used in telecom networks where phase or time-of-day synchronization is required and where each network device participates in the PTP protocol.

Because a boundary clock is used at every node in the chain between PTP Grandmaster and PTP Slave, there is reduction in time error accumulation through the network.

More About G.8275.1

The G.8275.1 must meet the following requirements:

- Non-participant devices, that is, devices that only forward PTP packets, and PTP transparent clocks are not allowed.
- The telecom grandmaster (T-GM) provides timing to all other devices on the network. It does not synchronize its local clock with any other network element other than the Primary Reference Time Clock (PRTC).
- The telecom time slave clock (T-TSC) synchronizes its local clock to another PTP clock (in most cases, the T-BC), and does not provide synchronization through PTP to any other device.
- The telecom boundary clock (T-BC) synchronizes its local clock to a T-GM or an upstream T-BC, and provides timing information to downstream T-BCs or T-TSCs. If at a given point in time there are no higher-quality clocks available to a T-BC to synchronize to, it may act as a grandmaster.

The following figure describes a sample G.8275.1 topology.

**Figure 5: A Sample G.8275.1 Topology**

### PTP Domain

A PTP domain is a logical grouping of clocks that communicate with each other using the PTP protocol. A single computer network can have multiple PTP domains operating separately, for example, one set of clocks synchronized to one time scale and another set of clocks synchronized to another time scale. PTP can run over either Ethernet or IP, so a domain can correspond to a local area network or it can extend across a wide area network.

The allowed domain numbers of PTP domains within a G.8275.1 network are between 24 and 43 (both inclusive).

### PTP Messages and Transport

The following PTP transport parameters are defined:

- For transmitting PTP packets, either the forwardable multicast MAC address (01-1B-19-00-00-00) or the non-forwardable multicast MAC address (01-80-C2-00-00-0E) must be used as the destination MAC address. The MAC address in use is selected on a per-port basis through the configuration. However, the non-forwardable multicast MAC address (01-80-C2-00-00-0E) will be used if no destination MAC is configured.

  The source MAC address is the interface MAC address.

- For receiving PTP packets, both multicast MAC addresses (01-80-C2-00-00-0E and 01-1B-19-00-00-00) are supported.

- The packet rate for Announce messages is 8 packets-per-second. For Sync, Delay-Req, and Delay-Resp messages, the rate is 16 packets-per-second.

- Signaling and management messages are not used.
PTP Modes

Two-Way Operation
To transport phase and time synchronization and to measure propagation delay, PTP operation must be two-way in this profile. Therefore, only two-way operation is allowed in this profile.

One-Step and Two-Step Clock Mode
Both one-step and two-step clock modes are supported in the G.8275.1 profile.
A slave port must be capable of receiving and processing messages from both one-step clocks and two-step clocks, without any particular configuration. However, the master supports only one-step mode.

PTP Clocks
Two types of ordinary clocks and boundary clocks are used in this profile:

Ordinary Clock (OC)
1. OC that can only be a grandmaster clock (T-GM). In this case, one PTP port will be used as a master port. The T-GM uses the frequency, 1PPS, and ToD input from an upstream grandmaster clock.

![Figure 6: Ordinary Clock As T-GM](image)

The T-GM master port is a fixed master port.

Boundary Clock (T-BC)
1. T-BC that can only be a grandmaster clock (T-GM).
2. T-BC that can become a master clock and can also be a slave clock to another PTP clock.

![Figure 7: Ordinary Clock As Slave Clock (T-TSC)](image)
If the BMCA selects a port on the T-BC to be a slave port, all other ports are moved into the master role or a passive state.

**Figure 8: Boundary Clock**

![Boundary Clock Diagram](image)

**PTP Ports**

A port can be configured to perform either fixed master or slave role or can be configured to change its role dynamically. If no role is assigned to a port, it can dynamically assume a master, passive, or slave role based on the BMCA.

A master port provides the clock to its downstream peers.

A slave port receives clock from an upstream peer.

A dynamic port can work either as a master or a slave based on the BMCA decision.

In Cisco’s implementation of the G.8275.1:

- OC clocks can support only fixed master or slave port.
- One PTP port can communicate with only one PTP peer.
- BC can have a maximum of 64 ports. Fixed slave ports are not supported on the BC.

Each PTP node and link can introduce asymmetry, which affects the adequate time/phase accuracy over the networks. Asymmetry in a network occurs when one-way-delay of forward path (referred as forward path delay) and reverse path (referred as reverse path delay) is different. The magnitude of asymmetry can be positive or negative depending upon the difference of forward and reverse path delays.

**Virtual Port Support on T-BC**

G.8275.1 introduces the concept of a virtual port on the T-BC. A virtual port is an external frequency, phase and time input interface on a T-BC, which can participate in the source selection.
Alternate BMCA

The BMCA implementation in G.8275.1 is different from that in the default PTP profile. The G.8275.1 implementation is called the Alternate BMCA. Each device uses the alternate BMCA to select a clock to synchronize to, and to decide the port states of its local ports.

Benefits

With upcoming technologies like LTE-TDD, LTE-A CoMP, LTE-MBSFN and Location-based services, eNodeBs (base station devices) are required to be accurately synchronized in phase and time. Having GNSS systems at each node is not only expensive, but also introduces vulnerabilities. The G.8275.1 profile meets the synchronization requirements of these new technologies.

Prerequisites for Using the G.8275.1 Profile

- PTP over Multicast Ethernet must be used.
- Every node in the network must be PTP aware.
- It is mandatory to have a stable physical layer frequency whilst using PTP to define the phase.
- Multiple active grandmasters are recommended for redundancy.

Restrictions for Using the G.8275.1 Profile

- PTP Transparent clocks are not permitted in this profile.
- Changing PTP profile under an existing clock configuration is not allowed. Different ports under the same clock cannot have different profiles. You must remove clock configuration before changing the PTP profile. Only removing all the ports under a clock is not sufficient.
- One PTP port is associated with only one physical port in this profile.
- There is no support for BDI and VLAN.
- Signaling and management messages are not used.
- PTP message rates are not configurable.
- Non-hybrid T-TSC and T-BC clock configurations are not supported.
- In default profile configuration, delay-asymmetry value is provided in the clock source command only. This restricts it to change the delay-asymmetry value with a complete reconfiguration of clock source command. The delay-asymmetry value should be considered as static and cannot be changed at run-time.

Configuring the G.8275.1 Profile

Note

To know more about the commands referenced in this module, see the Cisco IOS Interface and Hardware Component Command Reference or the Cisco IOS Master Command List.
Configuring Physical Frequency Source

For more information, see the Configuring Synchronous Ethernet ESMC and SSM section in the Clocking and Timing chapter of this book.

Creating a Master-Only Ordinary Clock

```
ptp clock ordinary domain 24
local-priority 1
priority2 128
clock-port master-port-1
master profile g8275.1
local-priority 1
transport ethernet multicast interface Gig 0/0/1
clock-port master-port-2
master profile g8275.1
```

**Note**

It is mandatory that when electrical ToD is used, the `utc-offset` command is configured before configuring the `tod R0`, otherwise there will be a time difference of approximately 37 seconds between the master and slave clocks.

The following example shows that the utc-offset is configured before configuring the ToD to avoid a delay of 37 seconds between the master and slave clocks:

```
ptp clock ordinary domain 0
utc-offset 37
tod R0 cisco
input 1pps R0
clock-port master master
transport ipv4 unicast interface Loopback0 negotiation
```

**Associated Commands**

- `ptp clock`
- `local-priority`
- `priority2`

Creating an Ordinary Slave

```
ptp clock ordinary domain 24
hybrid
clock-port slave-port
slave profile g8275.1
transport ethernet multicast interface Gig 0/0/0
delay-asymmetry 1000
```
Creating Dynamic Ports

Dynamic ports can be created when you do not specify whether a port is master or slave. In such cases, the BMC dynamically chooses the role of the port.

```
ptp clock boundary domain 24 hybrid
time-properties persist 600
utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
clock-port bc-port-1 profile g8275.1 local-priority 1
transport ethernet multicast interface Gig 0/0/0
delay-asymmetry 500
clock-port bc-port-2 profile g8275.1 local-priority 2
transport ethernet multicast interface Gig 0/0/1
delay-asymmetry -800
```

Configuring Virtual Ports

```
ptp clock boundary domain 24 hybrid
utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
virtual-port virtual-port-1 profile g8275.1 local-priority 1
input 1pps R0
input tod R0 ntp
```

Note

It is mandatory that when electrical ToD is used, the utc-offset command is configured before configuring the tod R0, otherwise there will be a time difference of approximately 37 seconds between the master and slave clocks.

Restrictions for Configuring Virtual Ports

- Virtual port configuration is not allowed under Ordinary Clocks.
- Virtual port configuration is not supported under non-hybrid T-BC cases.

Associated Commands

- `input`

Verifying the Local Priority of the PTP Clock

```
Router# show ptp clock dataset default
CLOCK [Boundary Clock, domain 24]
  Two Step Flag: No
  Clock Identity: 0x2A:0:0:0:58:67:F3:4
  Number Of Ports: 1
  Priority1: 128
  Priority2: 90
  Local Priority: 200
  Domain Number: 24
```
Verifying the Port Parameters

Router# show ptp port dataset port
PORT [MASTER]
Clock Identity: 0x49:BD:D1:0:0:0:0:0
Port Number: 0
Port State: Unknown
Min Delay Req Interval (log base 2): 42
Peer Mean Path Delay: 648518346341351424
Announce interval (log base 2): 0
Announce Receipt Timeout: 2
Sync Interval (log base 2): 0
Delay Mechanism: End to End
Peer Delay Request Interval (log base 2): 0
PTP version: 2
Local Priority: 1
Not-slave: True

Verifying the Foreign Master Information

Router# show platform software ptp foreign-master domain 24
PTPd Foreign Master Information:

Current Master: SLA
Port: SLA
Clock Identity: 0x74:A2:E6:FF:FE:5D:CE:3F
Clock Stream Id: 0
Priority1: 128
Priority2: 128
Local Priority: 128
Clock Quality:
  Class: 6
  Accuracy: Within 100ns
  Offset (Log Variance): 0x4E5D
Steps Removed: 1
Not-Slave: FALSE

Verifying Current PTP Time

Router# show platform software ptpd tod
PTPd ToD information:

Time: 01/05/70 06:40:59

Verifying the Virtual Port Status

Router# show ptp port virtual domain 24
VIRTUAL PORT (vp)
Status: down
Clock Identity: 0x74:A2:E6:FF:FE:5D:CE:3F
Port Number: 1
Clock Quality:
  Class: 6
  Accuracy: 0x21
  Offset (log variance): 0x4E5D
Steps Removed: 0
Priority1: 128
Priority2: 128
Local Priority: 128
Not-slave: False

G.8275.1 Deployment Scenario

The following example illustrates a possible configuration for a G.8275.1 network with two masters, a boundary clock and a slave. Let’s assume that master A is the primary master and B is the backup master.

**Figure 9: Topology for a Configuration Example**

The configuration on master clock A is:

```
ptp clock ordinary domain 24
clock-port master-port profile g8275.1
  transport ethernet multicast interface GigabitEthernet 0/0/0
```

The configuration on master clock B is:

```
ptp clock ordinary domain 25
clock-port master-port profile g8275.1
  transport ethernet multicast interface GigabitEthernet 0/1/0
```

The configuration on the boundary clock is:

```
ptp clock boundary domain 24 hybrid
  local-priority 3
clock-port slave-port-a profile g8275.1 local-priority 1
  transport ethernet multicast interface Gig 0/0/1
clock-port slave-port-b profile g8275.1 local-priority 2
  transport ethernet multicast interface Gig 0/1/1
clock-port master-port profile g8275.1
  transport Ethernet multicast interface Gig 0/2/1
```

The configuration on the slave clock is:
ptp clock ordinary domain 24 hybrid
clock-port slave-port slave profile g8275.1
transport Ethernet multicast interface Gig 0/0/0

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Interface and Hardware Component commands</td>
<td>Cisco IOS Interface and Hardware Component Command Reference</td>
</tr>
<tr>
<td>Clocking and Timing</td>
<td>Clocking and Timing</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.8275.1/Y.1369.1 (07/14)</td>
<td>SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS</td>
</tr>
<tr>
<td>G.8273.2/Y.1368.2 (05/14)</td>
<td>Packet over Transport aspects – Synchronization, quality and availability targets</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There are no new RFCs for this feature.</td>
</tr>
</tbody>
</table>

Feature Information for G.8275.1

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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.
Table 15: Feature Information for G.8275.1, on page 169 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

### Table 15: Feature Information for G.8275.1

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| G.8275.1–Support for 1588 profile     | XE 3.18  | This PTP telecom profile introduces phase and time synchronization with full timing support from the network. The following commands were introduced:  
  • local-priority  
  The following commands were modified:  
  • clock-port  
  • show ptp clock dataset default  
  • show ptp port dataset port  
  The following command is deprecated for the G.8275.1 profile clocks:  
  • show ptp port running  
  The alternate command is `show platform software ptp foreign-master [domain-number]`.  
  **Note** This command is applicable only for the G.8275.1 profile clocks. |
Tracing and Trace Management

This chapter contains the following sections:

- Tracing Overview, on page 171
- How Tracing Works, on page 172
- Tracing Levels, on page 172
- Viewing a Tracing Level, on page 173
- Setting a Tracing Level, on page 175
- Viewing the Content of the Trace Buffer, on page 175

Tracing Overview

Tracing is a function that logs internal events. Trace files are automatically created and saved to the trace logs directory on the hard disk: 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 system 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 trace log 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 172 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 16: Tracing Levels and Descriptions, on page 172 shows all of the trace levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

Table 16: Tracing Levels and Descriptions

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

Tracing and Trace Management
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 [uipod]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipod]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipod]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.398 [uipod]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipod]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipod]: (info): Going to send a status update to the shell manager in slot 0
08/23 11:53:47.417 [uipod]: (info): Going to send a status update to the shell manager in slot 0
```
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.
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, on page 179
- ODU and OTU, on page 179
- Deriving OTU1e and OTU2e Rates, on page 179
- OTU1e and OTU 2e Support on 8x10GE Interface Module, on page 180
- OTU3 Support in 2x40GE Interface Module, on page 181
- OTU4 Support on 1-port 100 Gigabit Ethernet Interface Module (1X100GE), on page 181
- Supported Transceivers, on page 181
- OTN Specific Functions, on page 181
- Standard MIBS, on page 182
- Restrictions for OTN, on page 182
- DWDM Provisioning, on page 183
- Configuring Transport Mode in 8x10GE and 2x40GE Interface Modules, on page 183
- Configuring Transport Mode in 1X100GE Interface Module, on page 186
- OTN Alarms, on page 188
- OTN Threshold, on page 191
- Configuring OTU Alarms, on page 193
- Configuring ODU Alarms, on page 193
- Configuring ODU Alarms, on page 193
- Loopback, on page 195
- Configuring Loopback, on page 195
- Forward Error Connection, on page 196
- SNMP Support, on page 199
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>
<thead>
<tr>
<th>G.709 Interface</th>
<th>Line Rate</th>
<th>Corresponding Ethernet Rate</th>
<th>Line Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTU-1e</td>
<td>11.0491 Gbit/s without stuffing bits</td>
<td>10 Gig E-LAN</td>
<td>10.3125 Gbit/s</td>
</tr>
<tr>
<td>G.709 Interface</td>
<td>Line Rate</td>
<td>Corresponding Ethernet Rate</td>
<td>Line Rate</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>-------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>OTU-2e</td>
<td>11.0957 Gbit/s without stuffing bits</td>
<td>10 Gig E-LAN</td>
<td>10.3125 Gbit/s</td>
</tr>
<tr>
<td>OTU-3</td>
<td>43.018 Gbit/s</td>
<td>STM-256 or OC-768</td>
<td>39.813 Gbit/s</td>
</tr>
</tbody>
</table>

**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 CPACK-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:
**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.

FECCMISMATCH 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:

```plaintext
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:

```plaintext
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
    2657188351 packets input, 170060465344 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 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 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
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
  ```
Verification of Enabled Ports for Controller Configuration

Use the show controllers command to verify the enabled 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, 1000000000 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 collisions, 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
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
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:

```bash
enable
cfg-term
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
```

---

Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE Fuji 16.9.x
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 BBER thresholds: ODU-SF = 10^-3  ODU-SD = 10^-6  OTU-SF = 10^-3  OTU-SD = 10^-6
TCA thresholds: SM = 10^-3  PM = 10^-3

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, 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
cfgurate terminal
cnoller dwdm 0/4/1
shut
```
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
```

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
```

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 (10GbE 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: ODU-SD-BER ODU-SF-BER ODU-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**
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR ASCII: AABBCCDD
- String OPERATOR HEX: AABBCCDD
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR HEX: AABBCCDD
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR HEX: AABBCCDD

**ODU TTI**
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR HEX: 11223344
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR HEX: 11223344
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR HEX: 11223344
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR HEX: 11223344
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR HEX: 11223344
- String SAPI ASCII: AABBCCDD
- String DAPI ASCII: AABBCCDD
- String OPERATOR HEX: 11223344
Configuring OTU Alerts

To configure OTU alerts:

```
Router#
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
no shutdown
end
```

Configuring ODU Alerts

To configure ODU alerts:

```
Router#
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
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

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:

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:

Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE Fuji 16.9.x
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:

```bash
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:

```bash
#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
```
### Forward Error Connection

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(corrected bits) = 856 < - This is the counter for Error alarms.
   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
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 [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 dwm 0/1/1
shutdown
g709 tti-processing enable
no shutdown
dn
```

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 dwm 0/1/1
shutdown
g709 tti-processing enable otu
```
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 : 0052414D455348000000000000052414D55348000
0000000000000000414242434344444000000000000000000000000

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. Unavailable Second occurs when there are 10 consecutive severely errored seconds.

Figure 12: 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 18: PM Parameters for OTN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBE-PM</td>
<td>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.</td>
</tr>
<tr>
<td>BBE-SM</td>
<td>Section Monitoring Background Block Errors (BBE-SM) indicates the number of background block errors recorded in the OTN section during the PM time interval.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BBER-PM</td>
<td>Path Monitoring Background Block Errors Ratio (BBER-PM) indicates the</td>
</tr>
<tr>
<td></td>
<td>background block errors ratio recorded in the OTN path during the PM time</td>
</tr>
<tr>
<td></td>
<td>interval.</td>
</tr>
<tr>
<td>BBER-SM</td>
<td>Section Monitoring Background Block Errors Ratio (BBER-SM) indicates the</td>
</tr>
<tr>
<td></td>
<td>background block errors ratio recorded in the OTN section during the PM</td>
</tr>
<tr>
<td></td>
<td>time interval.</td>
</tr>
<tr>
<td>ES-PM</td>
<td>Path Monitoring Errored Seconds (ES-PM) indicates the errored seconds</td>
</tr>
<tr>
<td></td>
<td>recorded in the OTN path during the PM time interval.</td>
</tr>
<tr>
<td>ESR-PM</td>
<td>Path Monitoring Errored Seconds Ratio (ESR-PM) indicates the errored</td>
</tr>
<tr>
<td></td>
<td>seconds ratio recorded in the OTN path during the PM time interval.</td>
</tr>
<tr>
<td>ESR-SM</td>
<td>Section Monitoring Errored Seconds Ratio (ESR-SM) indicates the errored</td>
</tr>
<tr>
<td></td>
<td>seconds ratio recorded in the OTN section during the PM time interval.</td>
</tr>
<tr>
<td>ES-SM</td>
<td>Section Monitoring Errored Seconds (ES-SM) indicates the errored seconds</td>
</tr>
<tr>
<td></td>
<td>recorded in the OTN section during the PM time interval.</td>
</tr>
<tr>
<td>FC-PM</td>
<td>Path Monitoring Failure Counts (FC-PM) indicates the failure counts</td>
</tr>
<tr>
<td></td>
<td>recorded in the OTN path during the PM time interval.</td>
</tr>
<tr>
<td>FC-SM</td>
<td>Section Monitoring Failure Counts (FC-SM) indicates the failure counts</td>
</tr>
<tr>
<td></td>
<td>recorded in the OTN section during the PM time interval.</td>
</tr>
<tr>
<td>SES-PM</td>
<td>Path Monitoring Severely Errored Seconds (SES-PM) indicates the severely</td>
</tr>
<tr>
<td></td>
<td>errored seconds recorded in the OTN path during the PM time interval.</td>
</tr>
<tr>
<td>SES-SM</td>
<td>Section Monitoring Severely Errored Seconds (SES-SM) indicates the severely</td>
</tr>
<tr>
<td></td>
<td>errored seconds recorded in the OTN section during the PM time interval.</td>
</tr>
<tr>
<td>SESR-PM</td>
<td>Path Monitoring Severely Errored Seconds Ratio (SESR-PM) indicates the</td>
</tr>
<tr>
<td></td>
<td>severely errored seconds ratio recorded in the OTN path during the PM</td>
</tr>
<tr>
<td></td>
<td>time interval.</td>
</tr>
</tbody>
</table>
**Definition**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESR-SM</td>
<td>Section Monitoring Severely Errored Seconds Ratio (SESR-SM) indicates the severely errored seconds ratio recorded in the OTN section during the PM time interval.</td>
</tr>
<tr>
<td>UAS-PM</td>
<td>Path Monitoring Unavailable Seconds (UAS-PM) indicates the unavailable seconds recorded in the OTN path during the PM time interval.</td>
</tr>
<tr>
<td>UAS-SM</td>
<td>Section Monitoring Unavailable Seconds (UAS-SM) indicates the unavailable seconds recorded in the OTN section during the PM time interval.</td>
</tr>
</tbody>
</table>

The following table shows the details of each type of PM parameter for FEC:

**Table 19: PM Parameters for FEC**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC</td>
<td>Bit Errors Corrected (BIEC) indicated the number of bit errors corrected in the DWDM trunk line during the PM time interval.</td>
</tr>
<tr>
<td>UC-WORDS</td>
<td>Uncorrectable Words (UC-WORDS) is the number of uncorrectable words detected in the DWDM trunk line during the PM time interval.</td>
</tr>
</tbody>
</table>

**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
- dBGI
• 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)
• dBBI

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:

```bash
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:

```bash
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:

```bash
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
BBER-SM-NE : 0 Threshold : 0 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 : 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
BBER-PM-NE : 0 Threshold : 0 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
BBER-SM-FE : 0 Threshold : 0 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
BBER-PM-FE : 0 Threshold : 0 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-NE : 0 0  ES-SM-FE : 0 0
ESR-SM-NE : 0.00000  ESR-SM-FE : 0.00000
SES-SM-NE : 0  SES-SM-NE : 0 0  SES-SM-FE : 0 0
SESR-SM-NE : 0.00000  SESR-SM-NE : 0.00000
UAS-SM-NE : 0  UAS-SM-FE : 0 0
BBE-SM-NE : 0  BBE-SM-NE : 0 0
BBER-SM-NE : 0.00000  BBER-SM-NE : 0.00000
FC-SM-NE : 0  FC-SM-NE : 0 0
ES-FM-NE : 0  ES-FM-NE : 0 0  ES-FM-FE : 0 0
ESR-FM-NE : 0.00000  ESR-FM-FE : 0.00000
SES-FM-NE : 0  SES-FM-FE : 0 0
SESR-FM-NE : 0.00000  SESR-FM-FE : 0.00000
UAS-FM-NE : 0  UAS-FM-FE : 0 0
BBE-FM-NE : 0  BBE-FM-NE : 0 0
BBER-FM-NE : 0.00000  BBER-FM-NE : 0.00000
FC-FM-NE : 0  FC-FM-NE : 0 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-FM-NE : 0  Threshold : 0  TCA(enable) : NO
ESR-FM-NE : 0.00000  Threshold : 0.00000  TCA(enable) : NO
SES-FM-NE : 0  Threshold : 0  TCA(enable) : NO
SESR-FM-NE : 0.00000  Threshold : 0.00000  TCA(enable) : NO
UAS-FM-NE : 0  Threshold : 0  TCA(enable) : NO
BBE-FM-NE : 0  Threshold : 0  TCA(enable) : NO
BBER-FM-NE : 0.00000  Threshold : 0.00000  TCA(enable) : NO
FC-FM-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-FM-FE : 0  Threshold : 0  TCA(enable) : NO
ESR-FM-FE : 0.00000  Threshold : 0.00000  TCA(enable) : NO
SES-FM-FE : 0  Threshold : 0  TCA(enable) : NO
SESR-FM-FE : 0.00000  Threshold : 0.00000  TCA(enable) : NO
UAS-FM-FE : 0  Threshold : 0  TCA(enable) : NO
BBE-FM-FE : 0  Threshold : 0  TCA(enable) : NO
BBER-FM-FE : 0.00000  Threshold : 0.00000  TCA(enable) : NO
FC-FM-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
SES-SM-FE :  0.00000  SES-SM-FE :  0.00000
UAS-SM-NE :  41  UAS-SM-FE :  0
BME-SM-NE :  0  BME-SM-FE :  0
BBER-SM-NE :  0.00000  BBER-SM-FE :  0.00000
ESR-PM-NE :  0.00000  ESR-PM-FE :  0.00000
SES-PM-NE :  0  SES-PM-FE :  0
SES-PM-FE :  0.00000  SES-PM-FE :  0.00000
UAS-PM-NE :  0  UAS-PM-FE :  0
BME-PM-NE :  3  BME-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.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link is not coming up</td>
<td>Perform shut and no shut actions of the interface.</td>
</tr>
<tr>
<td></td>
<td>Check for TTI Mismatch.</td>
</tr>
<tr>
<td></td>
<td>Verify the major alarms.</td>
</tr>
<tr>
<td></td>
<td>Verify the FEC mode.</td>
</tr>
<tr>
<td></td>
<td>Verify that Cisco supported transreceiver list is only used on both sides</td>
</tr>
<tr>
<td>Incrementing BIP Error</td>
<td>Verify FEC Mismatch.</td>
</tr>
<tr>
<td>FEC contains UC and EC errors and link is not coming up</td>
<td>Verify the FEC Mismatch.</td>
</tr>
</tbody>
</table>

**Associated Commands**

The following commands are used to configure OTN Wrapper:
<table>
<thead>
<tr>
<th>Commands</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td>Links</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
CHAPTER 13

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 13: 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 20: Type of SFPs for 1G and 10G Modules*

<table>
<thead>
<tr>
<th>Module</th>
<th>Optics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1G Module</td>
<td>SFP</td>
</tr>
<tr>
<td></td>
<td>CSFP</td>
</tr>
<tr>
<td>10G Module</td>
<td>SFP+</td>
</tr>
<tr>
<td></td>
<td>SFP</td>
</tr>
<tr>
<td></td>
<td>CSFP</td>
</tr>
</tbody>
</table>

- Operating Modes, on page 212
- SADT Mode, on page 214
- Bandwidth Mode, on page 214
- IOS Port Numbering, on page 218
- Supported Features on the Interface Module, on page 219
- Benefits, on page 219
- Restrictions, on page 219
- Configuring Interface Module, on page 219
- Configuring Bandwidth Mode, on page 228
- Interface Module Rules, on page 229
- Associated Commands, on page 243
- Additional References, on page 243

**Operating Modes**

The interface module supports the following two operating modes:

- Full Subscription
- Over Subscription
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 supported for 16 ports of 1 Gigabit Ethernet and 10GE bandwidth is supported for 10 Gigabit 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.
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 Priority 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

### SADT Mode

For more information on SADT mode, see [IP SLA—Service Performance Testing](#).

### Bandwidth Mode

Each interface module subslot can be assigned a bandwidth. You can reserve the slots with specific bandwidth so that the interface module that consumes more than the configured bandwidth is not used.

Note

The bandwidth mode is not supported on ASR 903 Routers and is only supported on ASR 907 Routers.

The following table shows the interface module slots for the bandwidth mode.

<table>
<thead>
<tr>
<th>IM Subslot</th>
<th>Bandwidth Mode</th>
<th>SADT Operating Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td>10</td>
<td>10 Gbps</td>
<td>XFI-Pass Through Mode</td>
</tr>
<tr>
<td>IM Subslot</td>
<td>Bandwidth Mode</td>
<td>SADT Operating Mode</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>1</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>XFI-Pass Through Mode</td>
</tr>
<tr>
<td>2</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>18 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>20 Gbps</td>
<td>XFI-Pass Through Mode</td>
</tr>
<tr>
<td>3</td>
<td>Not Available</td>
<td>NA</td>
</tr>
<tr>
<td>4</td>
<td>Not Available</td>
<td>NA</td>
</tr>
<tr>
<td>5</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>18 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>20 Gbps</td>
<td>XFI-Pass Through Mode</td>
</tr>
<tr>
<td>6</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>18 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td>7</td>
<td>80 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>100 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td>8</td>
<td>80 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>100 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td>9</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>18 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
</tbody>
</table>
## Slot Support on Operating Modes

The following table shows the slots supported on different operating modes on ASR 907 NCS 4216 Routers.

<table>
<thead>
<tr>
<th>IM Subslot</th>
<th>Bandwidth Mode</th>
<th>SADT Operating Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>18 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>20 Gbps</td>
<td>XFI-Pass Through Mode</td>
</tr>
<tr>
<td>11</td>
<td>Not Available</td>
<td>NA</td>
</tr>
<tr>
<td>12</td>
<td>Not Available</td>
<td>NA</td>
</tr>
<tr>
<td>13</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>18 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>20 Gbps</td>
<td>XFI-Pass Through Mode</td>
</tr>
<tr>
<td>14</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>18 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>20 Gbps</td>
<td>XFI-Pass Through Mode</td>
</tr>
<tr>
<td>15</td>
<td>8 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>Port Expansion Mode or XFI-Pass Through Mode</td>
</tr>
<tr>
<td></td>
<td>18 Gbps</td>
<td>Port Expansion Mode</td>
</tr>
<tr>
<td></td>
<td>20 Gbps</td>
<td>XFI-Pass Through Mode</td>
</tr>
<tr>
<td>IM Subslot</td>
<td>SADT Operating Mode</td>
<td>IM Operating Modes</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>0, 1</td>
<td>Port Expansion Mode</td>
<td>Unsupported</td>
</tr>
<tr>
<td></td>
<td>XFI-Pass Through Mode</td>
<td>8-port 1GE + 1-port 1GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8-port 1GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16-port 1GE Over Subscribed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18-port 1GE Over Subscribed</td>
</tr>
<tr>
<td>2, 5, 10, 13, 14, 15</td>
<td>XFI-Pass Through Mode</td>
<td>8-port 1GE + 1-port 10GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16-port 1GE + 1-port 10GE Over Subscribed</td>
</tr>
<tr>
<td></td>
<td>Any</td>
<td>8-port 1GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8-port 1GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16-port 1GE Over Subscribed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18-port 1GE Over Subscribed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-port 10GE</td>
</tr>
<tr>
<td>3, 4, 7, 8, 11, 12</td>
<td>Any</td>
<td>8-port 1GE + 1-port 10GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8-port 1GE + 1-port 1GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8-port 1GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-port 10GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16-port 1GE + 1-port 10GE Over Subscribed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16-port 1GE Over Subscribed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18-port 1GE Over Subscribed</td>
</tr>
<tr>
<td>6, 9</td>
<td>Any</td>
<td>8-port 1GE + 1-port 1GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8-port 1GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-port 10GE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16-port 1GE Over Subscribed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18-port 1GE Over Subscribed</td>
</tr>
</tbody>
</table>

The following table shows the slots supported for different operating modes for ASR 903 routers.
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

<table>
<thead>
<tr>
<th>IM Subslot</th>
<th>IM Operating Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 3, 4, and 5</td>
<td>16-port 1GE + 1-port 10GE Fully Subscribed</td>
</tr>
<tr>
<td></td>
<td>8-port 1GE + 1-port 10GE</td>
</tr>
<tr>
<td></td>
<td>18-port 1GE Fully Subscribed</td>
</tr>
<tr>
<td>1, 2</td>
<td>Unsupported</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1G Face Plate Port</th>
<th>SFP Optics</th>
<th>CSFP Optics</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Gigabit Ethernet 0/x/0</td>
<td>Gigabit Ethernet 0/x/0 and Gigabit Ethernet 0/x/1</td>
</tr>
<tr>
<td>1</td>
<td>Gigabit Ethernet 0/x/2</td>
<td>Gigabit Ethernet 0/x/2 and Gigabit Ethernet 0/x/3</td>
</tr>
<tr>
<td>2</td>
<td>Gigabit Ethernet 0/x/4</td>
<td>Gigabit Ethernet 0/x/4 and Gigabit Ethernet 0/x/5</td>
</tr>
<tr>
<td>3</td>
<td>Gigabit Ethernet 0/x/6</td>
<td>Gigabit Ethernet 0/x/6 and Gigabit Ethernet 0/x/7</td>
</tr>
<tr>
<td>4</td>
<td>Gigabit Ethernet 0/x/8</td>
<td>Gigabit Ethernet 0/x/8 and Gigabit Ethernet 0/x/9</td>
</tr>
<tr>
<td>5</td>
<td>Gigabit Ethernet 0/x/10</td>
<td>Gigabit Ethernet 0/x/10 and Gigabit Ethernet 0/x/11</td>
</tr>
<tr>
<td>6</td>
<td>Gigabit Ethernet 0/x/12</td>
<td>Gigabit Ethernet 0/x/12 and Gigabit Ethernet 0/x/13</td>
</tr>
<tr>
<td>7</td>
<td>Gigabit Ethernet 0/x/14</td>
<td>Gigabit Ethernet 0/x/14 and Gigabit Ethernet 0/x/15</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>10G Face Plate Port</th>
<th>SFP+</th>
<th>SFP (1G BW)</th>
<th>CSFP (1G BW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Ten Gigabit Ethernet 0/x/16</td>
<td>Ten Gigabit Ethernet 0/x/16</td>
<td>Ten Gigabit ethernet 0/x/16 and Gigabit Ethernet 0/x/17</td>
</tr>
</tbody>
</table>

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 only supported on Cisco ASR 900 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 all other control packets.

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
```
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 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 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 GigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
Example: Configuring Full Subscription Modes

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
Example: Configuring Full Subscription Modes

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 GigabitEthernet 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 GigabitEthernet 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(config)# 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
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
  ----  ----------------------  ------------------  --------  --------  --------
  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      -
```
<table>
<thead>
<tr>
<th>Slot</th>
<th>Cfg IM Type</th>
<th>Actual IM Type</th>
<th>Op State</th>
<th>Ad State</th>
<th>Op Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>18x1G-OS</td>
</tr>
<tr>
<td>0/1</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>18x1G-OS</td>
</tr>
<tr>
<td>0/2</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>16x1G+1x10G-OS</td>
</tr>
<tr>
<td>0/3</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>16x1G+1x10G</td>
</tr>
<tr>
<td>0/4</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>16x1G+1x10G-OS</td>
</tr>
<tr>
<td>0/5</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>16x1G+1x10G-OS</td>
</tr>
<tr>
<td>0/6</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>18x1G-OS</td>
</tr>
<tr>
<td>0/8</td>
<td>-</td>
<td>NCS4200-1H-FK</td>
<td>IS-NR</td>
<td>IS</td>
<td>-</td>
</tr>
<tr>
<td>0/9</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>18x1G-OS</td>
</tr>
<tr>
<td>0/10</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>16x1G+1x10G-OS</td>
</tr>
<tr>
<td>0/11</td>
<td>-</td>
<td>Empty</td>
<td>N/A</td>
<td>N/A</td>
<td>-</td>
</tr>
<tr>
<td>0/12</td>
<td>-</td>
<td>Empty</td>
<td>N/A</td>
<td>N/A</td>
<td>-</td>
</tr>
<tr>
<td>0/13</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>16x1G+1x10G-OS</td>
</tr>
<tr>
<td>0/14</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>16x1G+1x10G-OS</td>
</tr>
<tr>
<td>0/15</td>
<td>NCS4200-1T16G-PS</td>
<td>NCS4200-1T16G-PS</td>
<td>IS-NR</td>
<td>IS</td>
<td>16x1G+1x10G-OS</td>
</tr>
</tbody>
</table>

**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 traffic queue in Over Subscription mode.

```bash
Router# show platform hw-configuration
```

```
0/8 fpga dump 4
```

OS LP Drop 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  20-gbps
  0/2    A900-IMA8CS1Z-M  A900-IMA8CS1Z-M  IS-NR    IS       18x1G-OS  20-gbps
  0/3    A900-IMA8CS1Z-M  A900-IMA8CS1Z-M  IS-NR    IS       16x1G+1x10G 20-gbps
  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  20-gbps
  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 20-gbps
  0/11   -                -                Empty    N/A       -       -
  0/12   -                -                Empty    N/A       -       -
  0/13   A900-IMA8CS1Z-M  A900-IMA8CS1Z-M  IS-NR    IS       16x1G+1x10G-OS 20-gbps
  0/14   A900-IMA8CS1Z-M  A900-IMA8CS1Z-M  IS-NR    IS       16x1G+1x10G-OS 20-gbps
  0/15   A900-IMA8CS1Z-M  A900-IMA8CS1Z-M  IS-NR    IS       16x1G+1x10G-OS 20-gbps
#show platform hw-configuration
Slot  Cfg IM Type  Actual IM Type  Op State  Ad State  Op Mode
------  -------------------  -------------------  --------  --------  --------
  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 10-gbps
  0/2    NCS4200-1T16G-PS NCS4200-1T16G-PS  IS-NR    IS       18x1G 10-gbps
```

Use `show platform software agentiomd [IM module] fpga clear [port number]` to clear High Priority and Low Priority counters in Over Subscription mode.

```
#show platform software agentiomd 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
```
### Interface Module Rules

**NCS 4206 ASR 903 Routers or Cisco RSP3C-400-S Rules for A900-IMA8CS1Z NCS4200-1T16G-PS**

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed&lt;br&gt; • 16 x 1GigE (CSFP) + 1 x 10GigE (SFP+) Fully subscribed&lt;br&gt; • 18-port 1GE Fully subscribed</td>
<td>The IM cannot be in slot 0 if IMA1C is in slot 4</td>
</tr>
<tr>
<td>1</td>
<td>Not Supported</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>Not Supported</td>
<td>—</td>
</tr>
</tbody>
</table>
### Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not supported</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>Not supported</td>
<td>—</td>
</tr>
</tbody>
</table>
## Interface Module Rules

### Slot Number  | Supported IM Operating Modes | Restrictions
--- | --- | ---
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 | —
### Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| 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. |
## Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| 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.
## Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| 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 Oversubscribed or 1-port 10G Fully subscribed mode or 8-port 1G + 1-port 1G Fully subscribed mode.  
• If Slot 0 is in 8-port 1GE 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. |
<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| 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 subscibed mode, or 16-port 1G + 1-port 10G Over subscibed mode, then no IM can be present in slot 12.  
• If Slot 2 is in 8-port 1G + 1-port 10G Fully subscibed mode, or 16-port 1G + 1-port 10G Over subscibed 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) Oversubscribed  
              • 8-port 1GE + 1-port 1GE Fully subscribed  
              • 1-port 10G 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 subscibed, or 16-port 1G + 1-port 10G Over subscibed 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. |
### Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>• 8-port 1GE (SFP) Fully subscribed</td>
<td>• If Slot 6 is in 8-port 1GE fully subscribed, or 16-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.</td>
</tr>
<tr>
<td></td>
<td>• 16-port 1GE (CSFP) Oversubscribed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 18-port 1GE (CSFP) Oversubscribed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8-port 1GE + 1-port 1GE Fully subscribed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1-port 10 GE Fully subscribed</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>All modes are supported</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>All modes are supported</td>
<td>—</td>
</tr>
<tr>
<td>9</td>
<td>• 8-port 1GE (SFP) Fully subscribed</td>
<td>• If Slot 9 is in 8-port 1GE fully subscribed, or 16-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.</td>
</tr>
<tr>
<td></td>
<td>• 16-port/18-port 1GE (CSFP) Oversubscribed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 16-port 1GE (CSFP) Oversubscribed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8-port 1GE + 1-port 1GE Fully subscribed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1-port 10 GE Fully subscribed</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>• 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed</td>
<td>• If IM is in slot 10 then NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported.</td>
</tr>
<tr>
<td></td>
<td>• 16-port/18-port 1GE (CSFP) Oversubscribed</td>
<td>• If IM is in slot 10, then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported.</td>
</tr>
<tr>
<td></td>
<td>• 8-port 1GE+1-port 1GE Fully subscribed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1-port 10 GE Fully subscribed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8-port 1G Fully subscribed</td>
<td></td>
</tr>
<tr>
<td>Slot Number</td>
<td>Supported IM Operating Modes</td>
<td>Restrictions</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>11</td>
<td>All modes are supported</td>
<td></td>
</tr>
</tbody>
</table>
### Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 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).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the IM is in 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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, and no IM can be present in slot 1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If IM8Z or IMA2F is 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IF NCS4200-1T8S-10CS (5G_CEM) is in slot 11, then the IM in slot 15 is in only 8-port 1 GE Fully Subscribed, OR in 16/18-port 1GE Oversubscribed mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If NCS4200-48T1E1-CE is in slot 11, then the IM is in slot 15 is in only 8-port 1GE Fully Subscribed, or</td>
<td></td>
</tr>
</tbody>
</table>
## Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>in 16/18-port 1GE Oversubscribed mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
### Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>All modes are supported</td>
<td></td>
</tr>
</tbody>
</table>
### Interface Module Rules

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Supported IM Operating Modes</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If Slot 12 has IMA2Z, then slots 2 and 10 in 8-port 1GE Fully subscribed mode, or 16-port/18-port 1GE Oversubscribed mode or 1-port 10GE Fully subscribed mode or 8-port 1G + 1-port 1GE Fully subscribed mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Slot Number</td>
<td>Supported IM Operating Modes</td>
<td>Restrictions</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| 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 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.  
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 Oversubscribed 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 1G 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 Oversubscribed 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. |
### Associated Commands

The following table shows the Associated Commands for interface module configuration:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>dump fpga [port number]</td>
<td></td>
</tr>
<tr>
<td>clear fpga [port number]</td>
<td></td>
</tr>
</tbody>
</table>

### Additional References

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>
Related Topic | Document Title
--- | ---
Compact-SFP | Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>There are no standards and RFCs for this feature.</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>There are no MIBs for this feature. <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Card Protection for 48-Port T1/E1 CEM and 48-Port T3/E3 CEM Interface Modules

The Card Protection feature is introduced for the 48-Port T1/E1 and 48-port T3/E3 interface modules. In this feature, the interface module bay is protected by another interface module of the same type.

The Card Protection feature is required to protect traffic flow either when an interface module is out of service, when the software fails or a hardware component has issues. Because card protection is supported only on redundant interface modules, traffic is switched to the protect interface module when the active interface module does not respond, and vice-versa.

Note

This feature does not require any change in the patch panel of the interface modules.

In card protection, a Y Cable is used to multiplex the signal from the patch panel to both the ports of active and protect interface modules. Both ports receive the signal, but only the active interface module transmits the signal from its port.

Figure 14: Y Cable

To support the Card Protection feature, the configuration on the active and protect interface module must be same. To achieve this, a virtual interface module is created with the same interface module type as the active interface module. A virtual controller is also created, which broadcasts the configuration to both the interface modules. The configuration on the physical controllers is then blocked and you can make configuration changes only on the virtual controller. The user configuration can only be performed on the virtual controller.

The virtual controller supports CEM level configuration and all other configurations. These configurations are blocked on physical controllers.
DS3 (T3) channelized into T1 and E3 channelized into E1s are supported in card protection. For more information on configuration, see the Configuring the Controller of Channelized T3/T1 Interfaces section.

**Note**
- Y Cable, on page 246
- Card Protection Switchover, on page 246
- Restrictions, on page 247
- Supported Features on Interface Module, on page 247
- Configuring Maintenance Commands, on page 248
- Configuring T3/E3 Card Protection, on page 248
- Associated Commands, on page 252
- Additional References, on page 253

**Y Cable**

In card protection, a Y cable is used to multiplex the signal from the patch panel to both the ports of active and standby interface modules. Both the active and protect ports receive the signal, but only the active port transmits the signal from its port. Protect port transmitter is disabled.

**Card Protection Switchover**

The following table shows the card protection switchover trigger and time to complete the switchover between the working and protect interface module.

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Module Reload with CLI OIR</td>
<td>Less than 50 millisecond</td>
</tr>
<tr>
<td>Non-responsive Interface Module Process (interface module reloads on its own, the reload is initiated due to software error)</td>
<td>100 millisecond to 200 millisecond</td>
</tr>
<tr>
<td>Interface Module shuts down due to high temperature</td>
<td>Less than 50 millisecond</td>
</tr>
<tr>
<td>Interface Module shuts down using CLI</td>
<td>Less than 50 millisecond</td>
</tr>
<tr>
<td>Interface Module stops using CLI</td>
<td>Less than 50 millisecond</td>
</tr>
</tbody>
</table>
### Alarm Based Switchover

Alarm based switchover is only applicable for Loss Of Signal (LOS) alarm. Switchover happens only when the number of ports with LOS alarm in working interface module is greater than that on the protect interface module.

Each card protection group maintains a weight for each working and protect interface module. This weight is updated when the LOS alarms are asserted or cleared. The switchover happens only if the weight of working interface module and protect interface module stays same for a certain amount of time called soak time.

When there is any issue with the Patch Panel, both working interface module and protect interface module have the same number of LOS alarms (weights are same). Hence, switchover does not happen.

### Restrictions

- Card physical jack out convergence time for card protection switchover is more than 50 milliseconds.
- The time taken to restart the interface module due to any software error is more than 50 milliseconds.
- Alarm toggle on active or backup card causes at least one card protection switch.
- When BERT is started from the virtual controllers, the syslog displays the physical controllers instead of the virtual controller port.

### Supported Features on Interface Module

The supported features are:

- Switching Mode
  - Non-revertive mode
  - Revertive mode
- Alarm Based Switchover
- SerDes Based Switchover
- Adaptive Clock Recovery (ACR) on virtual CEM
- Differential Clock Recovery (DCR) on virtual CEM
Configuring Maintenance Commands

- Maintenance Commands
  - Lockout
  - Force
  - Manual

Note

All controller configurations are performed on the virtual controller.

You can create card protection with one slot (either primary or backup) and the remaining slots can be added later.

Configuring Maintenance Commands

To configure maintenance commands:

```
enable
configure terminal
card-protection 4
primary slot 0 bay 0
backup slot 0 bay 5
end
```

```
card-protection 4
card-protection [manual {backup|primary} | force {backup|primary} | lockout]
end
```

Priority Table

The following table shows the priority of the actions:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lockout</td>
</tr>
<tr>
<td>2</td>
<td>Force</td>
</tr>
<tr>
<td>3</td>
<td>Alarm or Card Failure</td>
</tr>
<tr>
<td>4</td>
<td>Manual Switch</td>
</tr>
<tr>
<td>5</td>
<td>Revert</td>
</tr>
</tbody>
</table>

Configuring T3/E3 Card Protection

Pre-requisites

The interface module should be free from any configuration.

Configuring Card Protection Group:
enable
configure terminal
card-protection {1-16}
primary slot 0 bay 0
backup slot 0 bay 5
end

Note
The card protection number 1 to 16 refers to the Card Protection Group Number (CPGN).

Note
This is a non-revertive mode.

Configuring Virtual Card and Virtual Controller:

When card protection group is configured, it creates virtual card for card protection object, denoted by 8/x/port. Slot 8 is a fixed slot number for all card protection-created virtual card. Bay number ‘x’ is derived from the CPGN, where x=CPGN-1. Since card protection group number ranges from 1 to 16, bay number ranges from 0 to 15. Virtual controllers can be configured from 8/x/0 to 8/x/47.

Physical Card Configuration:

Configures mode T3/E3 on physical controllers of both primary (0/0) and backup (0/5) card.

```
enable
configure terminal
controller mediatype 8/0/0
mode t3
end
```

Virtual Card Configuration:

- Configures mode T3/E3 on virtual controllers.
- Configures CEM on virtual controller (8/x/port).
- Configures xconnect and local connect on CEM interface.

```
enable
configure terminal
controller t3 8/0/0
cem 0 unframed
interface cem 8/0/0
cem 0
xconnect 11.1.1.1 112 encasulation mpls
end
```

Note
This is a non-revertive mode.

Note
To un-configure a CEM group under a virtual controller, first perform shutdown of the virtual controller and then un-configure the CEM group.
Configuring Revertive Mode

To configure revertive mode:

```
   enable
   configure terminal
   card-protection 4
   primary slot 0 bay 0
   backup slot 0 bay 5
   end
   card-protection 4
   revertive time [30-720]
   end
```

**Note**
The revertive time ranges from 30 to 720 seconds.

Verifying T3/E3 Card Protection Configuration

Use **show card-protection detail** command to verify card protection group configuration.

```
# show card-protection 2 detail
Working(0/1:A900-IMA48T-C NCS4200-48T3E3-CE):
   Number of LOS Alarms:7
   ok,Active
   1:1, Revertive

Protect(0/2:A900-IMA48T-C NCS4200-48T3E3-CE):
   Number of LOS Alarms:7
   ok,Inactive
   1:1, Revertive

Revert Timer : (Not Started)
Last switchover reason :None
```

```
# show card-protection 4
CPGN Primary Card Backup Card Active
-------------------------------------------------------------------------------
4 0/1 0/2 Primary
```

```
# show running-configuration
| b 8/0/0
controller mediatype 8/0/0
! controller mediatype 8/0/1
! controller mediatype 8/0/2
```

Use **show xconnect all** command to verify xconnect configuration.

```
# show xconnect all
XC ST=Xconnect State S1=Segment1 State S2=Segment2 State
UP=Up DN=Down AD=Admin Down IA=Inactive
SB=Standby HS=Hot Standby RV=Recovering NH=No Hardware
XC ST Segment 1 S1 Segment 2 S2
-------------------------------------------------------------------------------
UP pri ac CE8/0/0:0(SATOP T3) UP mpls 11.1.1.1:112 UP
```

Configuring T1/E1 Card Protection

Configuring Card Protection Group:

```plaintext
enable
configure terminal
card type t1 0 2
card type t1 0 1
card-protection [1-16]
primary slot 0 bay 1
backup slot 0 bay 2
end
```

The card protection number 1 to 16 refers to CPGN.

Configuring Virtual Card and Virtual Controller:

When card protection group is configured, it creates virtual card for card protection object, denoted by 8/x/port. Slot 8 is a fixed slot number for all card protection created virtual card. Bay number ‘x’ for virtual card is x =CPGN -1 = 15. Virtual controllers can be configured from 8/15/0 to 8/15/47.

Physical Card Configuration:

- No configuration is required for traffic.

Virtual Card Configuration:

- Configures CEM on virtual controller (8/x/port).
- Configures xconnect and local connect on CEM interface.

```plaintext
enable
configure terminal
controller t1 8/15/0
cem 0 unframed
interface cem 8/15/0
cem 0
xconnect 11.1.1.1 212 encasulation mpls
end
```

```plaintext
enable
configure terminal
controller t1 8/15/11
cem 0 unframed
interface cem 8/15/11
cem 0
connect testLC cem 8/15/0 0 cem 8/15/11 0
end
```

To un-configure a CEM group under a virtual controller, first perform shutdown of the virtual controller and then un-configure the CEM group.

Configuring Revertive Mode

To configure revertive mode:
enable
configure terminal

card-protection 4
primary slot 0 bay 0
backup slot 0 bay 5
end
card-protection 4
revertive time [30-720]
end

Note
The revertive time ranges from 30 to 720 seconds.

Verification of T1/E1 Card Protection Configuration

Use `show card-protection` command to verify card protection group configuration.

```
#show card-protection 2 detail
Working(0/1:A900-IMA48T-C NCS4200-48T1E1-CE):
   Number of LOS Alarms:7
   ok, Active
   1:1, Revertive

Protect(0/2:A900-IMA48T-C NCS4200-48T1E1-CE):
   Number of LOS Alarms:7
   ok, Inactive
   1:1, Revertive

Revert Timer : (Not Started)
Last switchover reason :None

Use `show xconnect all` command to verify xconnect configuration.

```
#show xconnect all | I CE8/15/
  UP   pri   ac CE8/15/0:0(SATOP T1) UP mpls 11.1.1.1:212 UP
#
#show xconnect all | i CE8/15/
  72   testLC CE8/15/11 SAT1 0 CE8/15/12 SAT1 0 UP
#
```

Associated Commands

The following table shows the commands for the IM configuration:

<table>
<thead>
<tr>
<th>Command</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Card Protection Creation Commands:</strong></td>
<td></td>
</tr>
<tr>
<td>card-protection <code>CPGN</code></td>
<td></td>
</tr>
<tr>
<td>card-protection `{primary</td>
<td>backup}`</td>
</tr>
<tr>
<td>card-protection revertive time</td>
<td></td>
</tr>
<tr>
<td><strong>Card Protection Maintenance Commands:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Compact-SFP</td>
<td>Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet</td>
</tr>
</tbody>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>There are no standards and RFCs for this feature.</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>There are no MIBs for this feature.</td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
CHAPTER 15

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.

By default, the 8X10GE interface 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.
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, tx0/4/0, 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, l2PhysIf: 0, l3PhysIf: 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_oid: 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, l2PhysIf: 0, l3PhysIf: 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, 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_oid: 0

### Configuring 10G Mode from 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 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

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, 12PhyIf: 0, 13PhyIf: 1, 13TDM: 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, 12PhyIf: 0, 13PhyIf: 1, 13TDM: 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):

<table>
<thead>
<tr>
<th>Commands</th>
<th>Links</th>
</tr>
</thead>
</table>
Overview of Over Subscription and Partial Port Modes on the 8-port 10 Gigabit Ethernet Interface Module

The 8-port 10 Gigabit Ethernet interface module (8X10GE) requires eight backplane XFI lines to the ASIC to operate efficiently. The chassis has different backplane capacity or bandwidth on each of its subslot. The 8X10GE interface module could only be used in subslots that offered the eight XFI backplane lines. The following table shows the slots that 8X10GE interface module support without over subscription mode:

<table>
<thead>
<tr>
<th>Slot No</th>
<th>Slot 0</th>
<th>Slot 1</th>
<th>Slot 2</th>
<th>Slot 3</th>
<th>Slot 4</th>
<th>Slot 5</th>
<th>Slot 6</th>
<th>Slot 7</th>
<th>Slot 8</th>
<th>Slot 9</th>
<th>Slot 10</th>
<th>Slot 11</th>
<th>Slot 12</th>
<th>Slot 13</th>
<th>Slot 14</th>
<th>Slot 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>8X10GE</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

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 number 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.
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 data rate.

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>
<thead>
<tr>
<th>Supported Features and Constraints</th>
<th>8X10 GE Over Subscription Mode</th>
<th>4 X10 G Partial Port Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Platforms</td>
<td>ASR 907 RSP3-400</td>
<td>ASR 907 RSP3-400</td>
</tr>
<tr>
<td>FPGA Mode</td>
<td>Supported only with XFI passthrough mode Minimum version 0.22</td>
<td>Supported on both XFI passthrough and port expansion mode</td>
</tr>
<tr>
<td>Subslots</td>
<td>Supported on only selected subslots</td>
<td>Supported on only selected subslots</td>
</tr>
</tbody>
</table>
### 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 24: Supported Subslots and SerDes Lines used by the 8X10GE Interface Module with Over Subscription Modes**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Supported Slots</th>
<th>SerDes Lines Used</th>
<th>Enabled Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:1 over subscription mode</td>
<td>3, 4, 11, 12</td>
<td>2, 3, 6, 7, 0, 1, 2, 3</td>
<td>All ports, 0, 1, 4, 5</td>
</tr>
<tr>
<td>4 Port Mode (Partial Port mode)</td>
<td>34</td>
<td>2, 3, 6, 7</td>
<td></td>
</tr>
</tbody>
</table>

**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.
Over subscription on the 8X10GE interface module is supported only with the XFI Passthrough mode.

The `license feature service-offload enable` command is used to change the FPGA mode to the XFI Passthrough 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.

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 25: Maximum Slot Population of the 8X10 GE Interface Module**

<table>
<thead>
<tr>
<th>Subslot</th>
<th>8X10 GE Interface Module Mode</th>
<th>Port Numbers</th>
<th>SerDes Numbers</th>
<th>ASIC No.</th>
<th>CNIS Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>4X10G Partial Port</td>
<td>0</td>
<td>27</td>
<td>ASIC-1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8X10G Fully Subscribed Mode</td>
<td>0</td>
<td>7</td>
<td>ASIC-1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subslot</td>
<td>8X10 GE Interface Module Mode</td>
<td>Port Numbers</td>
<td>SerDes Numbers</td>
<td>ASIC No.</td>
<td>CNIS Used</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------</td>
<td>--------------</td>
<td>---------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>12</td>
<td>4X10G Partial Port</td>
<td>4</td>
<td>11</td>
<td>ASIC-1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4X10G Partial Port</td>
<td>0</td>
<td>27</td>
<td>ASIC-0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>8X10G Fully Subscribed</td>
<td>0</td>
<td>7</td>
<td>ASIC-0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>4X10G Partial Port</td>
<td>4</td>
<td>11</td>
<td>ASIC-0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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(config)# hw-module 0/12 A900-IMA8Z mode 8x10G-2:1-OS
  ```

- **Example: Configuring 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
CHAPTER 16

Configuring the SDM Template

This section details the approximate number of resources supported in each template for a router running the license.

- Prerequisites for the SDM Template, on page 265
- Restrictions for the SDM Template, on page 265
- Information About the SDM Template, on page 267
- Selecting the SDM Template, on page 278
- Verifying the SDM Template, on page 280
- SDM Template Supported Features on RSP3 Module, on page 280

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.

Restrictions for the SDM Template

- 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 `sdmprefer` 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 `sdmprefer` 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.

<table>
<thead>
<tr>
<th>Release</th>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.6.1</td>
<td>49-50 mins</td>
<td>Reload to SSO bulk Sync state</td>
</tr>
<tr>
<td>16.7.1</td>
<td>50 mins</td>
<td>Reload to SSO bulk Sync state</td>
</tr>
<tr>
<td>16.8.1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>16.9.1</td>
<td>75 mins</td>
<td>Reload to SSO bulk Sync state</td>
</tr>
</tbody>
</table>
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 26: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP3)

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Default Template (RPF)</th>
<th>IPv4 Template (No RPF)</th>
<th>IPv6 Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table</td>
<td>200K</td>
<td>200K</td>
<td>200K</td>
</tr>
<tr>
<td>IPv4/VPNv4 Routes</td>
<td>Without MPLS</td>
<td>Without MPLS</td>
<td>Without MPLS</td>
</tr>
<tr>
<td></td>
<td>32k urpf ipv4 routes +</td>
<td>192k ipv4 routes</td>
<td>76k ipv4 routes</td>
</tr>
<tr>
<td></td>
<td>160k ipv4 routes</td>
<td>With MPLS</td>
<td>With MPLS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>32k urpf ipv4 routes +</td>
<td>192k (ipv4 routes + mpls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>160k (ipv4 routes + mpls</td>
<td>labels)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Labels = 32000</td>
<td>MPLS Labels = 32000</td>
</tr>
<tr>
<td>IPv6/VPNv6 Routes</td>
<td>8192</td>
<td>8192</td>
<td>36864</td>
</tr>
<tr>
<td>uRPF IPv4 routes</td>
<td>32768</td>
<td>32768</td>
<td>32768</td>
</tr>
<tr>
<td>IPv4 mcast routes</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>(mroutes)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 mcast routes</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>(mroutes)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bridge Domains</td>
<td>4094</td>
<td>4094</td>
<td>4094</td>
</tr>
<tr>
<td>EoMPLS Tunnels</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>MPLS VPN</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>VRF Lite</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>VPLS Instances</td>
<td>3500</td>
<td>3500</td>
<td>3500</td>
</tr>
<tr>
<td>IPv4 ACL entries</td>
<td>1000 (984 user</td>
<td>1000 (984 user</td>
<td>1000 (984 user</td>
</tr>
<tr>
<td></td>
<td>configurable)</td>
<td>configurable)</td>
<td>configurable)</td>
</tr>
<tr>
<td>IPv6 ACL entries</td>
<td>128 (124 user</td>
<td>128 (124 user</td>
<td>128 (124 user</td>
</tr>
<tr>
<td></td>
<td>configurable)</td>
<td>configurable)</td>
<td>configurable)</td>
</tr>
<tr>
<td>Functionality</td>
<td>Default Template (RPF )</td>
<td>IPv4 Template (No RPF)</td>
<td>IPv6 Template</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------</td>
<td>------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>v4 QoS Classifications</td>
<td>16000</td>
<td>16000</td>
<td>16000</td>
</tr>
<tr>
<td>v6 QoS Classifications</td>
<td>NS</td>
<td>NS</td>
<td>NS</td>
</tr>
<tr>
<td>Egress policers per ASIC</td>
<td>NS</td>
<td>NS</td>
<td>NS</td>
</tr>
<tr>
<td>OAM sessions</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>IPSLA sessions</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>EFP</td>
<td>16000</td>
<td>16000</td>
<td>16000</td>
</tr>
<tr>
<td>Maximum VLANs per port</td>
<td>4,000 per ASIC</td>
<td>4,000 per ASIC</td>
<td>4,000 per ASIC</td>
</tr>
<tr>
<td>Maximum VPLS neighbors</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Maximum attachment circuit per BD</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>STP Instances</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Maximum Etherchannel groups</td>
<td>48</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Maximum Interfaces per Etherchannel groups</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Maximum VRRP per system</td>
<td>255</td>
<td>255</td>
<td>255</td>
</tr>
<tr>
<td>Maximum HSRP per system</td>
<td>255</td>
<td>255</td>
<td>255</td>
</tr>
<tr>
<td>Maximum Ingress MPLS labels</td>
<td>32000</td>
<td>32000</td>
<td>32000</td>
</tr>
<tr>
<td>Maximum FRR/TE Headend</td>
<td>500</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>Maximum FRR/TE Midpoints</td>
<td>5000</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>Maximum E-LMI sessions</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Maximum BFD sessions</td>
<td>1023</td>
<td>1023</td>
<td>1023</td>
</tr>
<tr>
<td>Maximum SPAN/RSPAN sessions</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Maximum Queue counters per ASIC/system</td>
<td>40000/48000</td>
<td>40000/48000</td>
<td>40000/48000</td>
</tr>
<tr>
<td>Functionality</td>
<td>Default Template (RPF)</td>
<td>IPv4 Template (No RPF)</td>
<td>IPv6 Template</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Maximum Policer counters per ASIC/system</td>
<td>12000/24000</td>
<td>12000/24000</td>
<td>12000/24000</td>
</tr>
<tr>
<td>Max BDI for L3</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Multicast OIF per group for VF Lite or mVPN</td>
<td>255</td>
<td>255</td>
<td>255</td>
</tr>
<tr>
<td>Multicast OIF per group for native multicast</td>
<td>255</td>
<td>255</td>
<td>255</td>
</tr>
<tr>
<td>Queues per ASIC/system</td>
<td>40000/48000</td>
<td>40000/48000</td>
<td>40000/48000</td>
</tr>
<tr>
<td>Max Queues per EFP</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Ingress Classifications</td>
<td>16000</td>
<td>16000</td>
<td>16000</td>
</tr>
<tr>
<td>Egress Classifications</td>
<td>48000</td>
<td>48000</td>
<td>48000</td>
</tr>
<tr>
<td>Max Ingress Policers per ASIC/system</td>
<td>12000/24000</td>
<td>12000/24000</td>
<td>12000/24000</td>
</tr>
<tr>
<td>Max Egress Policers per ASIC/system</td>
<td>NS</td>
<td>NS</td>
<td>NS</td>
</tr>
<tr>
<td>Maximum EFPs per BD</td>
<td>256</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Maximum number of BDI for PW</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Maximum Layer 3 interfaces</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Max REP segments</td>
<td>NS</td>
<td>NS</td>
<td>NS</td>
</tr>
<tr>
<td>Maximum class-maps</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum policy maps</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Max number of OSPF Neighbors</td>
<td>400</td>
<td>400</td>
<td>400</td>
</tr>
<tr>
<td>Max number of ISIS neighbors</td>
<td>400</td>
<td>400</td>
<td>400</td>
</tr>
<tr>
<td>Max number of ISIS instances</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>Max number of BGP neighbors</td>
<td>250</td>
<td>250</td>
<td>250</td>
</tr>
</tbody>
</table>
### Information About the SDM Template

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Default Template (RPF)</th>
<th>IPv4 Template (No RPF)</th>
<th>IPv6 Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number IEEE 802.1ag/Y.1731(CFM) instances at 1 sec for xconnect</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Max number IEEE 802.1ag/Y.1731(CFM) instances at 3.3 ms for BD &amp; xconnect</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Max number IEEE 802.1ag/Y.1731(CFM) instances at 100 ms for BD &amp; xconnect</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Max number of Y.1731 instances</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum Class-maps in policy-map</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>Max number of match statements per class-map</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Max number of BFD sessions at 3.3 ms</td>
<td>1023</td>
<td>1023</td>
<td>1023</td>
</tr>
<tr>
<td>Max number of BFD sessions at 100 ms</td>
<td>1023</td>
<td>1023</td>
<td>1023</td>
</tr>
<tr>
<td>Max number of BFD sessions at 1 S</td>
<td>1023</td>
<td>1023</td>
<td>1023</td>
</tr>
<tr>
<td>Max number of IGP Prefixes protected via LFA-FRR</td>
<td>1500</td>
<td>1500</td>
<td>1500</td>
</tr>
<tr>
<td>Max number of L3VPN Prefixes protected via LFA-FRR</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>Max number of L2VPN sessions protected via LFA-FRR</td>
<td>2000</td>
<td>2000</td>
<td>2000</td>
</tr>
</tbody>
</table>

---

4 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 27: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP2)**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default Template</th>
<th>Video Template</th>
<th>IP Template</th>
<th>Maximum IPv6 QoS Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table</td>
<td>16000</td>
<td>16000</td>
<td>16000</td>
<td>16000</td>
</tr>
<tr>
<td>Virtual local area network (VLAN) mapping</td>
<td>4000</td>
<td>4000</td>
<td>65536</td>
<td>4000</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>20000</td>
<td>12000</td>
<td>24000</td>
<td>20000</td>
</tr>
<tr>
<td>IPv6 routes</td>
<td>3962</td>
<td>3962</td>
<td>1914</td>
<td>3962</td>
</tr>
<tr>
<td>VPNv4 routes</td>
<td>20000</td>
<td>12000</td>
<td>24000</td>
<td>20000</td>
</tr>
<tr>
<td>VPNv6 routes</td>
<td>3962</td>
<td>3962</td>
<td>1914</td>
<td>3962</td>
</tr>
<tr>
<td>IPv4 multicast routes (mroutes)</td>
<td>1000</td>
<td>2000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Layer 2 multicast groups</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Bridge Domains (BD)</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>MAC-in-MAC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ethernet over MPLS (EoMPLS) tunnels</td>
<td>2000</td>
<td>2000</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>MPLS Virtual Private Network (VPN)</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Virtual Routing and Forwarding (VRF) lite</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Access Control List (ACL) entries</td>
<td>2000</td>
<td>4000</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>Queues per Application-Specific Integrated Circuit (ASIC)</td>
<td>4095</td>
<td>4095</td>
<td>4095</td>
<td>4095</td>
</tr>
</tbody>
</table>
## Information About the SDM Template

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default Template</th>
<th>Video Template</th>
<th>IP Template</th>
<th>Maximum IPv6 QoS Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Quality of Service (QoS) classifications</td>
<td>4096</td>
<td>2048</td>
<td>4096</td>
<td>4096</td>
</tr>
<tr>
<td>Policers</td>
<td>4096</td>
<td>4096</td>
<td>4096</td>
<td>4096</td>
</tr>
<tr>
<td>Ethernet Operations, Administration, and Maintenance (OAM) sessions</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>IP Service Level Agreements (IPSLA) sessions</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Ethernet Flow Point (EFP)</td>
<td>8000</td>
<td>8000</td>
<td>8000</td>
<td>8000</td>
</tr>
<tr>
<td>Maximum VLANs per port</td>
<td>4094</td>
<td>4094</td>
<td>4094</td>
<td>4094</td>
</tr>
<tr>
<td>Maximum I-TAG per system</td>
<td>500</td>
<td>500</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>Maximum VPLS neighbors</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Maximum attachment circuit per BD</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>STP Instances</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Maximum Etherchannel groups</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Maximum Interfaces per Etherchannel groups</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Maximum Hot Standby Router Protocol (HSRP)</td>
<td>128 (For Cisco IOS-XE Release 3.14 and earlier)</td>
<td>128 (For Cisco IOS-XE Release 3.14 and earlier)</td>
<td>128 (For Cisco IOS-XE Release 3.14 and earlier)</td>
<td>128 (For Cisco IOS-XE Release 3.14 and earlier)</td>
</tr>
<tr>
<td></td>
<td>256 (For Cisco IOS-XE Release 3.15 and later)</td>
<td>256 (For Cisco IOS-XE Release 3.15 and later)</td>
<td>256 (For Cisco IOS-XE Release 3.15 and later)</td>
<td>256 (For Cisco IOS-XE Release 3.15 and later)</td>
</tr>
<tr>
<td>Resource</td>
<td>Default Template</td>
<td>Video Template</td>
<td>IP Template</td>
<td>Maximum IPv6 QoS Template</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Maximum Virtual Router Redundancy Protocol (VRRP)</td>
<td>128 (For Cisco IOS-XE Release 3.14 and earlier)</td>
<td>128 (For Cisco IOS-XE Release 3.14 and earlier)</td>
<td>128 (For Cisco IOS-XE Release 3.14 and earlier)</td>
<td>128 (For Cisco IOS-XE Release 3.14 and earlier)</td>
</tr>
<tr>
<td></td>
<td>255 (For Cisco IOS-XE Release 3.15 and later)</td>
<td>255 (For Cisco IOS-XE Release 3.15 and later)</td>
<td>255 (For Cisco IOS-XE Release 3.15 and later)</td>
<td>255 (For Cisco IOS-XE Release 3.15 and later)</td>
</tr>
<tr>
<td>Maximum Ingress MPLS labels</td>
<td>32000</td>
<td>32000</td>
<td>32000</td>
<td>32000</td>
</tr>
<tr>
<td>Maximum Egress MPLS labels</td>
<td>28500</td>
<td>28500</td>
<td>28500</td>
<td>28500</td>
</tr>
<tr>
<td>Maximum Fast Reroute (FRR)/Traffic Engineering (TE) headend</td>
<td>500</td>
<td>500</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>Maximum FRR/TE midpoints</td>
<td>5000</td>
<td>5000</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>Maximum Enhanced Local Management Interface (E-LMI) sessions</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum Bidirectional Forwarding Detection (BFD) sessions</td>
<td>1023</td>
<td>1023</td>
<td>1023</td>
<td>1023</td>
</tr>
<tr>
<td>Maximum Switched Port Analyzer (SPAN)/Remote SPAN (RSPAN) sessions</td>
<td>32</td>
<td>32</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Maximum Queue counters (packet &amp; byte)</td>
<td>65536</td>
<td>65536</td>
<td>65536</td>
<td>65536</td>
</tr>
<tr>
<td>Maximum Policer counters (packet &amp; byte)</td>
<td>49152</td>
<td>49152</td>
<td>49152</td>
<td>49152</td>
</tr>
<tr>
<td>Maximum number of BDI for Layer 3</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
</tbody>
</table>
Using IPv4 and VPNv4 routes concurrently reduces the maximum scaled value as both the routes use the same TCAM space.

Due to label space limitation of 16000 VPNv4 routes, to achieve 24000 VPNv4 routes in IP template use per VRF mode.

Using Layer 2 and Layer 3 multicast groups concurrently reduces the scale number to 1947.

ACLs contend for TCAM resources with Multicast Virtual Private Network (MVPN).

User available queues are 1920.

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 28: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP1A)

<table>
<thead>
<tr>
<th>Resource</th>
<th>IP template</th>
<th>Video template</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table</td>
<td>16000</td>
<td>16000</td>
</tr>
<tr>
<td>Virtual local area network (VLAN) mapping</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>24000</td>
<td>12000</td>
</tr>
<tr>
<td>IPv6 routes</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>VPNv4 routes</td>
<td>24000</td>
<td>12000</td>
</tr>
<tr>
<td>VPNv6 routes</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>IPv4 multicast routes (mroutes)</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>Layer 2 multicast groups</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>Bridge Domains (BD)</td>
<td>4094</td>
<td>4094</td>
</tr>
<tr>
<td>MAC-in-MAC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ethernet over MPLS (EoMPLS) tunnels</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>MPLS Virtual Private Network (VPN)</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Resource</td>
<td>IP template</td>
<td>Video template</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Virtual Routing and Forwarding (VRF) lite</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Virtual Private LAN Services (VPLS) instances</td>
<td>26</td>
<td>26</td>
</tr>
<tr>
<td>Access Control List (ACL) entries(^6)</td>
<td>2000</td>
<td>4000</td>
</tr>
<tr>
<td>Queues per Application-Specific Integrated Circuit (ASIC) (^7)</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td>IPv4 Quality of Service (QoS) classifications</td>
<td>4096</td>
<td>2048</td>
</tr>
<tr>
<td>Policers</td>
<td>1024</td>
<td>1024</td>
</tr>
<tr>
<td>Ethernet Operations, Administration, and Maintenance (OAM) sessions</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>IP Service Level Agreements (IPSLA) sessions</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Ethernet Flow Point (EFP)</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>Maximum VLANs per port</td>
<td>4094</td>
<td>4094</td>
</tr>
<tr>
<td>Maximum I-TAG per system</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>Maximum VPLS neighbors</td>
<td>62</td>
<td>62</td>
</tr>
<tr>
<td>Maximum attachment circuit per BD</td>
<td>62</td>
<td>62</td>
</tr>
<tr>
<td>STP Instances</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Maximum Etherchannel groups</td>
<td>26</td>
<td>26</td>
</tr>
<tr>
<td>Maximum Interfaces per Etherchannel groups</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Maximum Hot Standby Router Protocol (HSRP)/Virtual Router Redundancy Protocol (VRRP)</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Maximum Ingress MPLS labels</td>
<td>16000</td>
<td>16000</td>
</tr>
<tr>
<td>Maximum Egress MPLS labels</td>
<td>28500</td>
<td>28500</td>
</tr>
<tr>
<td>Maximum Fast Reroute (FRR)/Traffic Engineering (TE) headend</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>Maximum FRR/TE midpoints</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>Maximum Enhanced Local Management Interface (E-LMI) sessions</td>
<td>1000</td>
<td>1000</td>
</tr>
</tbody>
</table>
Using IPv4 and VPNv4 routes concurrently reduces the maximum scaled value as both the routes use the same TCAM space.

User available routes are 3967.

Due to label space limitation of 16000 VPNv4 routes, to achieve 24000 VPNv4 routes in IP template use per VRF mode.

Using Layer 2 and Layer 3 multicast groups concurrently reduces the scale number to 1947.

ACLs contend for TCAM resources with Multicast Virtual Private Network (MVPN).

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 29: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP1B)

<table>
<thead>
<tr>
<th>Resource</th>
<th>VPNv4/v6 template</th>
<th>Video template</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table</td>
<td>256000</td>
<td>256000</td>
</tr>
<tr>
<td>IVLAN mapping</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>EVLAN mapping</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>Maximum VLANS per port</td>
<td>4094</td>
<td>4094</td>
</tr>
<tr>
<td>Maximum security addresses per EFP</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum security addresses per BD</td>
<td>10000</td>
<td>10000</td>
</tr>
<tr>
<td>Maximum security addresses</td>
<td>256000</td>
<td>256000</td>
</tr>
<tr>
<td>Maximum security configuration</td>
<td>256000</td>
<td>256000</td>
</tr>
<tr>
<td>EFPs per BD</td>
<td>62</td>
<td>62</td>
</tr>
<tr>
<td>Resource</td>
<td>VPNv4/v6 template</td>
<td>Video template</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>80000</td>
<td>80000</td>
</tr>
<tr>
<td>IPv6 routes</td>
<td>40000</td>
<td>80000</td>
</tr>
<tr>
<td>Maximum BD interfaces</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum ITAG per system</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>IPv4 routing groups</td>
<td>2000 (17)</td>
<td>80000</td>
</tr>
<tr>
<td>IPv6 routing groups</td>
<td>2000 (18)</td>
<td>80000</td>
</tr>
<tr>
<td>IPv4 multicast groups</td>
<td>2000 (19)</td>
<td>10000</td>
</tr>
<tr>
<td>IPv6 multicast groups</td>
<td>2000 (20)</td>
<td>10000</td>
</tr>
<tr>
<td>BDs</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>MAC-in-MAC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EoMPLS tunnels</td>
<td>8000</td>
<td>80000</td>
</tr>
<tr>
<td>MPLS VPN</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Virtual Routing and Forwarding Scale (VRFS)</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>VPLS instances</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum VPLS neighbors</td>
<td>62</td>
<td>62</td>
</tr>
<tr>
<td>ACL entries</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>IPv6 ACL entries</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Queues per ASIC</td>
<td>16384</td>
<td>16384</td>
</tr>
<tr>
<td>Classifications</td>
<td>12288</td>
<td>12288</td>
</tr>
<tr>
<td>Ingress policers per ASIC</td>
<td>8192</td>
<td>8192</td>
</tr>
<tr>
<td>Egress policers per ASIC</td>
<td>4096</td>
<td>4096</td>
</tr>
<tr>
<td>Maximum class maps</td>
<td>4096</td>
<td>4096</td>
</tr>
<tr>
<td>Maximum policy maps</td>
<td>1024</td>
<td>1024</td>
</tr>
<tr>
<td>Maximum queue counters</td>
<td>65536</td>
<td>65536</td>
</tr>
<tr>
<td>Maximum policer counters</td>
<td>48152</td>
<td>48152</td>
</tr>
<tr>
<td>OAM sessions</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>ELMI sessions</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>SLA sessions</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>EFPs</td>
<td>8000</td>
<td>8000</td>
</tr>
<tr>
<td>MPLS ingress labels</td>
<td>64000</td>
<td>64000</td>
</tr>
<tr>
<td>MPLS egress labels</td>
<td>80000</td>
<td>80000</td>
</tr>
<tr>
<td>FRR TE headend</td>
<td>1000</td>
<td>1000</td>
</tr>
</tbody>
</table>
### Selecting the SDM Template

To select an SDM template, complete the following steps:

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. `sdm prefer {default | video | ip | mvpn_rsp1a | VPNv4/v6 | max-ipv6-acl | enable_8k_efp | enable_copp | ipv4 | ipv6 | efp_feat_ext | enable_8k_efp | enable_copp | enable_l3vpn_cm | enable_l3vpn_cm | enable_match_inner_dscp | enable_portchannel_qos_multiple_active | vpls_stats_enable}

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>`sdm prefer {default</td>
<td>video</td>
</tr>
<tr>
<td></td>
<td>• default—Balances all functions.</td>
</tr>
<tr>
<td></td>
<td>• video—Increases multicast routes and ACLs.</td>
</tr>
<tr>
<td></td>
<td>• ip—Increases IPv4/VPNv4 routes. This option is available only on RSP1A.</td>
</tr>
<tr>
<td></td>
<td>• mvpn_rsp1a—Supports MVPN. This option is available only on RSP1A.</td>
</tr>
<tr>
<td></td>
<td>• VPNv4/v6—Increases IPv4/VPNv4 routes. This option is available only on RSP1B.</td>
</tr>
<tr>
<td></td>
<td>• max-ipv6-acl—Supports IPv6 QoS ACL routes. The NEQ Layer 4 operation is supported in maximum IPv6 QoS ACL template.</td>
</tr>
<tr>
<td></td>
<td>• ipv4—Enables the IPv4 template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td></td>
<td>• ipv6—Enables the IPv6 feature template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td></td>
<td>• efp_feat_ext—Enables the EFP feature template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td></td>
<td>• enable_8k_efp—Enables the 8K EFP feature template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td></td>
<td>• enable_copp—Enables the COPP feature template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td></td>
<td>• enable_l3vpn_cm—Enables the L3VPN conditional marking feature template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td></td>
<td>• enable_match_inner_dscp—Enables the match inner dscp feature template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td></td>
<td>• enable_portchannel_qos_multiple_active—Enables the port channel QoS multiple active feature template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td></td>
<td>• vpls_stats_enable—Enables the VPLS statistics feature template. This is supported on the RSP3 module.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# sdm prefer default</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note** When changing the SDM template, the router waits for two minutes before reloading. Do not perform any operation till the router reloads.
Verifying the SDM Template

You can use the following show commands to verify configuration of your SDM template:

- **show sdm prefer current**—Displays information about the active SDM template.

  Following is a sample output using the `show sdm prefer current` command to display the current template configured on the router:

  ```
  Router# show sdm prefer current
  The current template is "video" template.
  
  Router# show sdm prefer current
  The current template is "max-ipv6-qos" 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 following templates.

<table>
<thead>
<tr>
<th>SDM Template</th>
<th>Supported Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sdm prefer vpls_stats_enable</code></td>
<td>VPLS Statistics</td>
</tr>
<tr>
<td><code>sdm prefer efp_feat_ext</code></td>
<td>Split-Horizon Groups</td>
</tr>
<tr>
<td><code>sdm prefer enable_8k_efp</code></td>
<td>8K EFP (4 Queue Model)</td>
</tr>
<tr>
<td><code>sdm prefer enable_match_inner_dscp</code></td>
<td>Match Inner DSCP</td>
</tr>
<tr>
<td><code>sdm prefer enable_copp</code></td>
<td>Control Plane Policing</td>
</tr>
<tr>
<td><code>sdm prefer enable_portchannel_qos_multiple_active</code></td>
<td>QoS Support on Port Channel LACP Active Active 16K EFP Support on Port Channel</td>
</tr>
<tr>
<td><code>sdm prefer ipv4_ipv6</code></td>
<td>Enhance uRPF scale to 32K</td>
</tr>
</tbody>
</table>
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=metroaggservices,all:ASR-903;

Restrictions for Split-Horizon Groups on the RSP3 Module

- 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 are not configured, the total EFPs supported are 4K.

- EFPs configured on the same bridge domain and same split-horizon group, cannot forward to or recieve traffic from each other.
- We do not recommnd(configuration of Y.1564 and split-horizon group on the same EFP.
- We do not recommend configuring MAC security with split-horizon group.
- Split-horizon group is not supported for CFM on this template. Configuring split-horizon groups on CFM based MEPs may result in MEPs being unlearnt, 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 re-learn of traffic with new MAC address.

Following are known behavoirof 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.

<table>
<thead>
<tr>
<th>Split-Horizon Group</th>
<th>RSP3-400</th>
<th>RSP3-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default (No config)</td>
<td>4K EFP</td>
<td>2K EFP</td>
</tr>
<tr>
<td>Group 0</td>
<td>2K EFP</td>
<td>1K EFP</td>
</tr>
<tr>
<td>Group 1</td>
<td>2K EFP</td>
<td>1K EFP</td>
</tr>
</tbody>
</table>

Note: If Split-horizon configuration does not exist, number of EFPs supported are reduced to 4K EFPs.

| Note: Port-channel scale is half the regular scale of the EFP. |

**Configuring Split-Horizon Group on the RSP3 Module**

```bash
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 ASR 903 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-map 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 `sdmprefer enable_8k_efp`.
- Reset the SDM template using the CLI `sdmprefer disable_8k_efp`.

Restrictions for 8000 (8K) EFP

- 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 EFP Template

Below is the sample configuration to enable 8K EFP or 4 Queue mode template. On enabling `sdmprefer enable_8k_efp`, the router reloads and boots up with 8K EFP template.

```
RSP3-903(config)#sdmprefer 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.
Configuring the SDM Template

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)
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 up to 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.

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
```

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
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
```
## 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 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 on the RSP3

- sdm prefer enable_copp template must be enabled on the 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Total</th>
<th>Up</th>
<th>AdminDo</th>
<th>Down</th>
<th>ErrorDi</th>
<th>Unknown</th>
<th>Deleted</th>
<th>BdAdmDo</th>
</tr>
</thead>
<tbody>
<tr>
<td>bdomain</td>
<td>8000</td>
<td></td>
<td>8000</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xconnect</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>local sw</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>other</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>all</td>
<td>8000</td>
<td></td>
<td>8000</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Associated interface: port-channel 11

<table>
<thead>
<tr>
<th>Field</th>
<th>Total</th>
<th>Up</th>
<th>AdminDo</th>
<th>Down</th>
<th>ErrorDi</th>
<th>Unknown</th>
<th>Deleted</th>
<th>BdAdmDo</th>
</tr>
</thead>
<tbody>
<tr>
<td>bdomain</td>
<td>8000</td>
<td></td>
<td>8000</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xconnect</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>local sw</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>other</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>all</td>
<td>8000</td>
<td></td>
<td>8000</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
• 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 sdm prefer enable_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, IGMP are not supported.

• Only CPU destined Unicast Layer3 protocols packets are matched as part of COPP classification.

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 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.

<table>
<thead>
<tr>
<th>Supported Protocols</th>
<th>Criteria</th>
<th>Match</th>
<th>Queue#</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP - Trivial FTP</td>
<td>Port Match</td>
<td>IP access list ext cott-system-acl-tftp permit udp any any eq 69</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>TELNET</td>
<td>Port Match</td>
<td>IP access list ext cott-system-acl-telnet permit tcp any any eq telnet</td>
<td>NQ_CPU_CONTROL_Q</td>
</tr>
<tr>
<td>NTP - Network Time Protocol</td>
<td>Port Match</td>
<td>IP access list ext cott-system-acl-ntp permit udp any any eq ntp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>FTP - File Transfer Protocol</td>
<td>Port Match</td>
<td>IP access list ext cott-system-acl-ftp permit tcp host any any eq ftp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>Criteria</td>
<td>Match</td>
<td>Queue#</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>SNMP - Simple Network Management Protocol</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-snmp&lt;br&gt;permit udp any eq snmp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>TACACS - Terminal Access Controller Access-Control System</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-tacacs&lt;br&gt;permit tcp any tacacs</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>FTP-DATA</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-ftpdata&lt;br&gt;permit tcp any eq 20</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>HTTP - Hypertext Transfer Protocol</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-http&lt;br&gt;permit tcp any eq www</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>WCCP - Web Cache Communication Protocol</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-wccp&lt;br&gt;permit udp any eq 2048&lt;br&gt;any eq 2048</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>SSH - Secure Shell</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-ssh&lt;br&gt;permit tcp any eq 22</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>ICMP - Internet Control Message Protocol</td>
<td>Protocol Match</td>
<td>IP access list copp-system-acl-icmp&lt;br&gt;permit icmp any</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>DHCP - Dynamic Host Configuration Protocol</td>
<td>Port Match</td>
<td>IP access list copp-system-acl-dhcp&lt;br&gt;permit udp any eq bootps</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>MPLS- OAM</td>
<td>Port Match</td>
<td>IP access list copp-system-acl-mplsoam&lt;br&gt;permit udp any eq 3503&lt;br&gt;any</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
</tbody>
</table>
| LDP - Label Distribution Protocol | Port Match | IP access list copp-system-acl-ldp<br>permit udp any eq 646<br>any eq 646<br>permit tcp any eq 646 | NQ_CPU_CFQ
### 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.

---

### 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 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

! 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.

```sh
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.

```sh
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.

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
(pktx 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
(pktx 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
(pktx 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

```bash
Class-map match-any dscp
Match dscp af13
exit
policy-map matchdscp
Class dscp
Police cir 1000000
end
```

### Verifying Match Inner DSCP on RSP3 Module

```bash
Router# show platform hardware pp active feature qos resource-summary 0
PE1#res
RSP3 QoS Resource Summary

<table>
<thead>
<tr>
<th>Type</th>
<th>Total</th>
<th>Used</th>
<th>Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS TCAM</td>
<td>1024</td>
<td>0</td>
<td>1024</td>
</tr>
<tr>
<td>VOQs</td>
<td>49152</td>
<td>408</td>
<td>48744</td>
</tr>
<tr>
<td>QoS Policers</td>
<td>32768</td>
<td>0</td>
<td>32768</td>
</tr>
<tr>
<td>QoS Policier Profiles</td>
<td>1023</td>
<td>0</td>
<td>1023</td>
</tr>
<tr>
<td>Ingress CoS Marking Profiles</td>
<td>16</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>Egress CoS Marking Profiles</td>
<td>16</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>Ingress Exp &amp; QoS-Group Marking Profiles</td>
<td>64</td>
<td>3</td>
<td>61</td>
</tr>
<tr>
<td>Ingress QoS LPM Entries</td>
<td>32768</td>
<td>0</td>
<td>32768</td>
</tr>
</tbody>
</table>
```