The specifications and information regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

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

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice. In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

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

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

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

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

© 2017 Cisco Systems, Inc. All rights reserved.
CONTENTS

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
Password Recovery 15
Powering Off the Router 16
Finding Support Information for Platforms and Cisco Software Images 16
Using Cisco Feature Navigator 17
Using Software Advisor 17
Using Software Release Notes 17
<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Console Port Telnet and SSH Handling</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Console Port Overview</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Connecting Console Cables</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Installing USB Device Drivers</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Console Port Handling Overview</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Telnet and SSH Overview</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Persistent Telnet and Persistent SSH Overview</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Configuring a Console Port Transport Map</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Examples</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Configuring Persistent Telnet</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Examples</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Configuring Persistent SSH</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Examples</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Viewing Console Port, SSH, and Telnet Handling Configurations</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Important Notes and Restrictions</td>
<td>32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Configuring the Route Switch Processor</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuring Timing Ports</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Configuring the Management Ethernet Port</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Configuring Console Ports</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Reloading the Route Switch Processor</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Forcing a Route Switch Processor Switchover</td>
<td>34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Configuring Clocking and Timing</th>
<th>35</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clocking and Timing Restrictions</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Restrictions on RSP3 Module</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Clocking and Timing Overview</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Understanding PTP</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Telecom Profiles</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>PTP Redundancy</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>PTP Redundancy Using Hop-By-Hop Topology Design</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Best Master Clock Algorithm</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Hybrid Clocking</td>
<td>45</td>
</tr>
</tbody>
</table>
Verifying Interface Module Status 122
Configuring LAN/WAN-PHY Controllers 123
   Restrictions for LAN/WAN-PHY Mode 124
   Configuring LAN-PHY Mode 124
   Configuring WAN-PHY Mode 125
   Configuring the Flag for Path Trace 127
   Configuring WAN-PHY Error Thresholds 129
Configuration Examples 130
   Example: Basic Interface Configuration 130
   Example: MTU Configuration 131
   Example: VLAN Encapsulation 132

CHAPTER 8
Using the Management Ethernet Interface 133
   Gigabit Ethernet Management Interface Overview 133
   Gigabit Ethernet Port Numbering 133
   IP Address Handling in ROMmon and the Management Ethernet Port 134
   Gigabit Ethernet Management Interface VRF 134
   Common Ethernet Management Tasks 135
      Viewing the VRF Configuration 135
      Viewing Detailed VRF Information for the Management Ethernet VRF 135
      Setting a Default Route in the Management Ethernet Interface VRF 136
      Setting the Management Ethernet IP Address 136
      Telnetting over the Management Ethernet Interface 136
      Pinging over the Management Ethernet Interface 136
      Copy Using TFTP or FTP 137
      NTP Server 137
      SYSLOG Server 137
      SNMP-related services 137
      Domain Name Assignment 137
      DNS service 138
      RADIUS or TACACS+ Server 138
      VTY lines with ACL 138

CHAPTER 9
Configuring T1/E1 Interfaces 139
Configuration Tasks 139

Limitations 139

Required Configuration Tasks 140
  Setting the Card Type 140
  Configuring the Controller 141
  Verifying Controller Configuration 143

Optional Configurations 143
  Configuring Framing 143
  Setting an IP Address 145
  Configuring Encapsulation 146
  Configuring the CRC Size for T1 Interfaces 147
  Configuring a Channel Group 149
  Saving the Configuration 150

Troubleshooting E1 and T1 Controllers 150
  Setting Loopbacks 150

Running Bit Error Rate Testing 152

Monitoring and Maintaining the T1/E1 Interface Module 154

AIS on Core Failure 154
  Limitations of AIS 154
  Core Failure Event Detection 155
  Configuring AIS for Core Failure 155
  Verifying AIS Configuration 155
  Example: AIS Trigger 156

Verifying the Interface Configuration 156
  Verifying Per-Port Interface Status 156

Configuration Examples 157
  Example: Framing and Encapsulation Configuration 157
  Example: CRC Configuration 157
  Example: Facility Data Link Configuration 158
  Example: Invert Data on the T1/E1 Interface 158

CHAPTER 10

Configuring Optical Interface Modules 159

Limitations and Restrictions 159

Configuring the Controller 160
Configuring SDH 161
   Configuring SDH Mode 161
      SDH T1 Mode 161
      SDH T1 Mode 165
   Configuring SDH in POS Mode 168
   Configuring SONET Mode 169
   Configuring SONET Mode 169
   Configuring SONET Mode 169
   Configuring SONET POS Mode 171
   Configuring a CEM group 173
      Configuring CEM Group in SONET Mode 173
      Configuring CEM Group in SDH Mode 175
   Configuring DS3 Clear Channel on OC-3 and OC-12 Interface Module 176
      Configuring DS3 Clear Channel in SONET Mode 177
      Configuring DS3 Clear Channel in SDH Mode 179
Optional Configurations 181
   Configuring the National Bit 181
      Verifying the National Bit 181
   Configuring the CRC Size for T1 182
Optional Packet over SONET Configurations 182
   Encapsulation 183
   MTU Value 183
   CRC Value 183
   Keepalive Value 183
   Bandwidth 183
   Scrambling 184
   C2 Flag 184
   J1 Flag 184
Managing Interface Naming 184
   Identifying Slots and Subslot 184
Configuring Multilink Point-to-Point Protocol 185
   MLPPP Configuration Guidelines 185
   Creating a Multilink Bundle 185
   Assigning an Interface to a Multilink Bundle 186
Configuring Fragmentation Size and Delay on an MLPPP Bundle 187
Changing the Default Endpoint Discriminator 188
Disabling Fragmentation on an MLPPP Bundle 188
Configuring BERT 189
Configuring Automatic Protection Switching 189
TU-AIS Alarms 189
  Restrictions for TU-AIS Alarms 190
  Configuring TU-AIS Alarms 190
  Verification of TU-AIS Alarm Configuration 190
  Core Failure Event Detection 191
Verifying Interface Configuration 191
  Verifying Per-Port Interface Status 191
Troubleshooting 191
  Framing and Encapsulation Configuration Example 192
  National Bit Configuration Example 193
  CRC Configuration Example 193
  Facility Data Link Configuration Example 194
  MLPPP Configuration Example 194
  MFR Configuration Example 195
Configuration Examples 196
  Example of Cyclic Redundancy Check Configuration 196
  Example of Facility Data Link Configuration 196
  Example of Invert Data on T1/E1 Interface 196
Additional Resources 196

CHAPTER 11
Configuring Serial Interfaces 199
Information About Serial Interface Module 199
Restrictions 200
How to Configure Serial Interface 201
  Required Configuration Tasks 201
    Configuring the Controller 201
  Optional Configurations 202
    Configuring Layer 1 on Async Interface 202
    Configuring a Channel Group 204
CHAPTER 17

Configuring the SDM Template 293
Prerequisites for the SDM Template 293
Restrictions for the SDM Template 293
Information About the SDM Template 295
Selecting the SDM Template 306
Verifying the SDM Template 308

SDM Template Supported Features on RSP3 Module 308
VPLS Statistics 309
Split Horizon Enhancements on the RSP3 Module 310
Prerequisites for Split-Horizon Groups on the RSP3 Module 310
Restrictions for Split-Horizon Groups on the RSP3 Module 310
Split-Horizon Supported Scale 311
Configuring Split-Horizon Group on the RSP3 Module 311

8K EFP (4 Queue Model) 312
Information About 8000 (8K) EFP 312
Prerequisites for 8000 (8K) EFP 312
Restrictions for 8000 (8K) EFP 312
Configuring 8K Model 312
16K EFP Support on Port Channel 315
Restrictions for 16K EFP on Port Channel 316
Configuring 16K EFP on Port Channel 316
Verifying 16k EFP on Port Channel 316
Control Plane Policing 317
Restrictions for Control Plane Policing 317
Restrictions for CoPP on the RSP3 317
Supported Protocols 318
Input Rate-Limiting and Silent Mode Operation 320
How to Use Control Plane Policing 320
Configuration Examples for Control Plane Policing 322
Verification Examples for CoPP 322
QoS Support on Port Channel LACP Active Active 323
Benefits of QoS Support on Port Channel LACP Active Active 323
Restrictions for QoS Support on Port Channel LACP Active Active 323
Configuring QoS Support on Port Channel Active Active 323
Verification of QoS Support on Port Channel LACP Active Active 324
Match Inner DSCP on RSP3 Module 326
Restrictions for Match Inner DSCP on RSP3 Module 326
Configuring Match Inner DSCP on RSP3 Module 326
Verifying Match Inner DSCP on RSP3 Module 326

CHAPTER 18
Tracing and Trace Management 327
Tracing Overview 327
How Tracing Works 328
Tracing Levels 328
Viewing a Tracing Level 329
Setting a Tracing Level 331
Viewing the Content of the Trace Buffer 331

CHAPTER 19
Configuring and Monitoring Alarm 333
Monitoring Alarms 333
Network Administrator Checks Console or Syslog for Alarm Messages 334
   Enabling the Logging Alarm Command 334
   Examples of Alarm Messages 334
   ALARMS for Router 334
   Reviewing and Analyzing Alarm Messages 338
Configuring External Alarm Trigger 338
   Approaches for Monitoring Hardware Alarms 339
      Onsite Network Administrator Responds to Audible or Visual Alarms 339
   How to Configure External Alarms 339
      Example 340
Alarm Filtering Support 341
   Information About Alarm Filtering Support 341
      Overview of Alarm Filtering Support 341
      Prerequisites for Alarm Filtering Support 342
      Restrictions for Alarm Filtering Support 342
   How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications 343
      Configuring Alarm Filtering for Syslog Messages 343
      Configuring Alarm Filtering for SNMP Notifications 343
   Configuration Examples for Alarm Filtering Support 343
      Configuring Alarm Filtering for Syslog Messages: Example 343
      Configuring Alarm Filtering for SNMP Notifications: Example 343

CHAPTER 20

OTN Wrapper Overview 345
   Advantages of OTN 347
   ODU and OTU 347
   Deriving OTU1e and OTU2e Rates 347
   OTU1e and OTU 2e Support on 8x10GE Interface Module 348
   OTU3 Support in 2x40GE Interface Module 349
   OTU4 Support on 1-port 100 Gigabit Ethernet Interface Module (1X100GE) 349
   Supported Transceivers 349
   OTN Specific Functions 349
   Standard MIBS 350
   Restrictions for OTN 350
   DWDM Provisioning 351
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 1: Accessing and Exiting Command Modes

<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 <strong>logout</strong> command.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>From user EXEC mode, use the <strong>enable</strong> EXEC command.</td>
<td>Router#</td>
<td>To return to user EXEC mode, use the <strong>disable</strong> command.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>From privileged EXEC mode, use the <strong>configure terminal</strong> privileged EXEC command.</td>
<td>Router(config)#</td>
<td>To return to privileged EXEC mode from global configuration mode, use the <strong>exit</strong> or <strong>end</strong> command.</td>
</tr>
<tr>
<td>Interface configuration</td>
<td>From global configuration mode, specify an interface using an <strong>interface</strong> command.</td>
<td>Router(config-if)#</td>
<td>To return to global configuration mode, use the <strong>exit</strong> 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:

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

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

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”:

5. When your 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 console session, enter the quit command as shown in the following example:

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.

Note

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

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

Using Telnet to Access a Console Interface

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

**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$^1$</td>
<td>Move the cursor back one character</td>
</tr>
<tr>
<td>Ctrl-F or the Right Arrow key$^1$</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 3: History Substitution Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P or the Up Arrow key</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 key</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>?</td>
<td>Lists all commands available for a particular command mode.</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>
<tbody>
<tr>
<td>Router&gt; <code>enable</code> Password: &lt;password&gt; Router#</td>
<td>Enter the <code>enable</code> command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a “#” from the “&gt;”; for example, Router&gt; to Router# .</td>
</tr>
<tr>
<td>Router# <code>configure terminal</code></td>
<td>Enter the <code>configure terminal</code> privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)# .</td>
</tr>
<tr>
<td><code>interface gigabitEthernet ?</code></td>
<td>Enter interface configuration mode by specifying the serial interface that you want to configure using the <code>interface serial</code> global configuration command.</td>
</tr>
<tr>
<td><code>interface gigabitEthernet 0/0/0</code></td>
<td>Enter <code>?</code> 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.</td>
</tr>
<tr>
<td><code>interface gigabitEthernet 0/0/0</code></td>
<td>When the <code>&lt;cr&gt;</code> symbol is displayed, you can press Enter to complete the command.</td>
</tr>
<tr>
<td><code>interface gigabitEthernet 0/0/0</code></td>
<td>You are in interface configuration mode when the prompt changes to Router(config-if)# .</td>
</tr>
</tbody>
</table>
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>
<tbody>
<tr>
<td>Router(config-if)# ?</td>
<td>Interface configuration commands:</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>keepalive</td>
</tr>
<tr>
<td></td>
<td>lan-name</td>
</tr>
<tr>
<td></td>
<td>llc2</td>
</tr>
<tr>
<td></td>
<td>load-interval</td>
</tr>
<tr>
<td></td>
<td>calculation for an</td>
</tr>
<tr>
<td></td>
<td>locaddr-priority</td>
</tr>
<tr>
<td></td>
<td>logging</td>
</tr>
<tr>
<td></td>
<td>loopback</td>
</tr>
<tr>
<td></td>
<td>interface</td>
</tr>
<tr>
<td></td>
<td>mac-address</td>
</tr>
<tr>
<td></td>
<td>mls</td>
</tr>
<tr>
<td></td>
<td>mtu</td>
</tr>
<tr>
<td></td>
<td>netbios</td>
</tr>
<tr>
<td></td>
<td>or enable</td>
</tr>
<tr>
<td></td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>nrzi-encoding</td>
</tr>
<tr>
<td></td>
<td>ntp</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td>Router(config-if)#</td>
<td></td>
</tr>
</tbody>
</table>
**Command**

<table>
<thead>
<tr>
<th>Router(config-if)# ip ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface IP configuration subcommands:</td>
</tr>
<tr>
<td>access-group Specify access control for packets</td>
</tr>
<tr>
<td>accounting Enable IP accounting on this interface</td>
</tr>
<tr>
<td>address Set the IP address of an interface</td>
</tr>
<tr>
<td>authentication authentication subcommands</td>
</tr>
<tr>
<td>bandwidth-percent Set EIGRP bandwidth limit</td>
</tr>
<tr>
<td>broadcast-address Set the broadcast address of an interface</td>
</tr>
<tr>
<td>cgmp Enable/disable CGMP</td>
</tr>
<tr>
<td>directed-broadcast Enable forwarding of directed broadcasts</td>
</tr>
<tr>
<td>dvmrp DVMRP interface commands</td>
</tr>
<tr>
<td>hello-interval Configures IP-EIGRP hello interval</td>
</tr>
<tr>
<td>helper-address Specify a destination address for UDP broadcasts</td>
</tr>
<tr>
<td>hold-time Configures IP-EIGRP hold time</td>
</tr>
<tr>
<td>.</td>
</tr>
<tr>
<td>Router(config-if)# ip</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>secondary Make this IP address a secondary address</td>
</tr>
<tr>
<td>&lt;cr&gt;</td>
</tr>
<tr>
<td>Router(config-if)# ip address 172.16.0.1 255.255.255.0</td>
</tr>
</tbody>
</table>

**Comment**

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.

Enter the command that you want to configure for the interface. This example uses the **ip address** command.

Enter ? to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword.

A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

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.

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 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:

```bash
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ip address 172.16.0.1 255.255.255.0</td>
<td>In this example, Enter is pressed to complete the command.</td>
</tr>
</tbody>
</table>

Router(config-if)#
The `copy` command can be used to backup startup configuration files. Below are some examples showing the startup configuration file in NVRAM being backed up:

**Example 1: Copying Startup Configuration File to Bootflash**

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

**Example 2: Copying Startup Configuration File to USB Flash Disk**

Router# dir usb0:
Directory of usb0:/
43261 -rwx 208904396 May 27 2008 14:10:20 -07:00 asr903rpi1-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 asr903rpi1-adventerprisek9.02.01.00.122-33.XNA.bin
43262 -rwx 3172 Jul 2 2008 15:40:45 -07:00 startup-config 255497216 bytes total (40186880 bytes free)

**Example 3: Copying Startup Configuration File to a TFTP Server**

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

For more detailed information on managing configuration files, see the *Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S*.
Filtering Output from the show and more Commands

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

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

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

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

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

Password Recovery

⚠️ Warning
You will lose the startup configuration by using this Password Recovery procedure.

📝 Note
The configuration register is usually set to 0x2102 or 0x102. If you can no longer access the router (because of a lost login or TACACS password), you can safely assume that your configuration register is set to 0x2102.

Before you begin

Make sure that the hyperterminal has the following settings:

- 9600 baud rate
- No parity
- 8 data bits
- 1 stop bit
- No flow control

Step 1
Use the power switch to turn off the router, and then turn it on again.

Step 2
Press `Break` on the terminal keyboard within 60 seconds of power up to put the router into ROMMON. In some cases `Ctrl+Break` key combination can be used.
Step 3  Type `confr eg 0x2142` at the ROMMON.

1> confr eg 0x2142
1> sync

(This step bypasses the startup configuration where the passwords are stored.)

Step 4  Type `reset` at the ROMMON.

2> reset

The router reboots, but ignores the saved configuration.

Step 5  The router reloads and prompts for configuration. Type `no` after each setup question, or press Ctrl-C to skip the initial setup procedure.

Step 6  Type `enable` at the `Router>` prompt.

You are now in enable mode and should see the `Router#` prompt.

Step 7  Reset the config-register from 0x2142 to 0x2102. To do so, type the following:

```
config-register configuration_register_setting
```

Where, `configuration_register_setting` is 0x2102. For example,

```
hostname(config)#config-register 0x2102
```

---

### 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.
CHAPTER 2

Console Port Telnet and SSH Handling

This chapter covers the following topics:

- Console Port Overview, on page 19
- Connecting Console Cables, on page 19
- Installing USB Device Drivers, on page 19
- Console Port Handling Overview, on page 20
- Telnet and SSH Overview, on page 20
- Persistent Telnet and Persistent SSH Overview, on page 20
- Configuring a Console Port Transport Map, on page 21
- Configuring Persistent Telnet, on page 23
- Configuring Persistent SSH, on page 25
- Viewing Console Port, SSH, and Telnet Handling Configurations, on page 29
- Important Notes and Restrictions, on page 32

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 ASR 900 Series 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 ASR 900 Series 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 23 and the Configuring Persistent SSH, on page 25.
Configuring a Console Port Transport Map

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

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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates and names a transport map for handling console connections, and enter transport map configuration mode.</td>
</tr>
<tr>
<td><strong>transport-map type console transport-map-name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# transport-map type console</td>
<td></td>
</tr>
<tr>
<td>consolehandler</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>
</tr>
<tr>
<td>**connection wait [allow interruptible</td>
<td>none]**</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• <strong>none</strong>—The console connection immediately enters diagnostic mode.</td>
</tr>
<tr>
<td>Router(config-tmap)# connection wait none</td>
<td></td>
</tr>
</tbody>
</table>

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

Command or Action

**Step 5**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`banner [diagnostic</td>
<td>wait] banner-message`</td>
</tr>
</tbody>
</table>

- **diagnostic**—Creates a banner message seen by users directed into diagnostic mode as a result of the console transport map configuration.
- **wait**—Creates a banner message seen by users waiting for the IOS vty to become available.
- **banner-message**—The banner message, which begins and ends with the same delimiting character.

**Example:**

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

**Example:**

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

**Example:**

```bash
--Welcome to Diagnostic Mode--
```

**Example:**

```bash
X
```

**Example:**

```bash
Router(config-tmap)#
```

**Step 6**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits transport map configuration mode to re-enter global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router(config-tmap)# exit
```

**Step 7**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>transport type console console-line-number input transport-map-name</code></td>
<td>Applies the settings defined in the transport map to the console interface.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router(config)# transport type console 0 input consolehandler
```

The `transport-map-name` for this command must match the `transport-map-name` defined in the `transport-map type console` command.

---

### Examples

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

```bash
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'.
```

**Example:**

```bash
Welcome to diagnostic mode
```

**Example:**

```bash
X
```

**Example:**

```bash
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
```

**Example:**

```bash
Waiting for IOS vty line
```

**Example:**

```bash
X
```
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> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</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# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>transport-map type persistent telnet transport-map-name</code></td>
<td>Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# transport-map type persistent telnet telnethandler</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>connection wait [allow {interruptible}] [none {disconnect}]</code></td>
<td>Specifies how a persistent Telnet connection will be handled using this transport map:</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-tmap)# connection wait none</td>
<td>• allow—The Telnet connection waits for an IOS vty line to become available, and exits the router if interrupted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Example: | • **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:**  
Router(config-tmap)# banner diagnostic X  
**Example:**  
Enter TEXT message. End with the character 'X'.  
**Example:**  
--Welcome to Diagnostic Mode--  
**Example:**  
X  
**Example:**  
Router(config-tmap)#  
**Example:**  
(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS vty line as a result of the persistent Telnet configuration.  
• **diagnostic**—creates a banner message seen by users directed into diagnostic mode as a result of the persistent Telnet configuration.  
• **wait**—creates a banner message seen by users waiting for the vty line to become available.  
• **banner-message**—the banner message, which begins and ends with the same delimiting character. |

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

**Step 7**  
**exit**  
**Example:**  
Router(config-tmap)# exit  
Exits transport map configuration mode to re-enter global configuration mode. |
### 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.

```bash
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic 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
### 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>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode.</td>
</tr>
<tr>
<td><code>transport-map type persistent ssh transport-map-name</code></td>
<td>Example:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# transport-map type persistent ssh sshhandler</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies how a persistent SSH connection will be handled using this transport map:</td>
</tr>
<tr>
<td>`connection wait [allow {interruptible}</td>
<td>none {disconnect}]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Note Users can interrupt a waiting connection by entering Ctrl-C or Ctrl-Shift-6.</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><code>rsa keypair-name rsa-keypair-name</code></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 <strong>ip ssh rsa keypair-name</strong> command, do not apply to persistent SSH connections.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>No rsa-keypair-name is defined by default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-tmap)# rsa keypair-name sshkeys</td>
</tr>
</tbody>
</table>
### Configuring Persistent SSH

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>authentication-retries &lt;number-of-retries&gt;</td>
<td>(Optional) Specifies the number of authentication retries before dropping the connection. The default number-of-retries is 3.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-tmap)# authentication-retries 4</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>banner [diagnostic</td>
<td>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></td>
<td></td>
<td>diagnostic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wait</td>
</tr>
<tr>
<td></td>
<td></td>
<td>banner-message</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-tmap)# banner diagnostic X</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Enter TEXT message.  End with the character 'X'</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>--Welcome to Diagnostic Mode--</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>X</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-tmap)#</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>time-out &lt;timeout-interval&gt;</td>
<td>(Optional) Specifies the SSH time-out interval in seconds. The default timeout-interval is 120 seconds.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-tmap)# time-out 30</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>transport interface type num</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></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-tmap)# transport interface gigabitethernet 0</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>exit</td>
<td>Exits transport map configuration mode to re-enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-tmap)# exit</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>transport type persistent ssh input transport-map-name</td>
<td>Applies the settings defined in the transport map to the Management Ethernet interface. The transport-map-name for this command must match the transport-map-name defined in the transport-map type persistent ssh command.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# transport type persistent ssh input sshhandler</code></td>
<td></td>
</tr>
</tbody>
</table>
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
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
   Interface:
   Connection:
      Wait option: Wait Allow Interruptable
      Wait banner:
      Waiting for the IOS CLI
      Bshell banner:
      Welcome to Diagnostic Mode
Router# show transport-map name sshhandler
Transport Map:
   Name: sshhandler
   Type: Persistent SSH Transport
   Interface: GigabitEthernet0
   Connection:
Wait option: Wait Allow Interruptable
Wait banner:
Waiting for IOS prompt
Bshell banner:
Welcome to Diagnostic Mode
SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys
Router#

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

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

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

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

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

**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.
CHAPTER 3

Configuring the Route Switch Processor

This chapter describes how to configure the Route Switch Processor (RSP) on the Cisco ASR 900 Series Router and contains the following sections:

- Configuring Timing Ports, on page 33
- Configuring the Management Ethernet Port, on page 33
- Configuring Console Ports, on page 33
- Reloading the Route Switch Processor, on page 33
- Forcing a Route Switch Processor Switchover, on page 34

Configuring Timing Ports

For information about configuring timing ports on the RSP, see Chapter 1, “Configuring Clocking and Timing.”

Configuring the Management Ethernet Port

For information about configuring the management Ethernet port on the RSP, see Chapter 1, “Using the Management Ethernet Interface.”

Configuring Console Ports

For information about configuring console ports, see Chapter 1, “Console Port, Telnet, and SSH Handling.”

Reloading the Route Switch Processor

Use the following command in privileged EXEC mode:
### Table 6: Route Switch Processor Reload

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`hw-module slot number {logging</td>
<td>reload [force]</td>
</tr>
</tbody>
</table>

#### Note
The command is used to reload the standby RSP module. Use the `show platform` command to find active/standby slot number.

#### Note
The above task does not apply to Cisco ASR 902 router.

---

## Forcing a Route Switch Processor Switchover

To force the standby RSP to assume the role of the active RSP, use the `redundancy force-switchover` command in privileged EXEC mode.

```
Router# redundancy force-switchover
```

#### Note
The above task does not apply to Cisco ASR 902 router.

#### Note
Router should be in hot standby state for executing this command. This can be verified by using the show redundancy command.
CHAPTER 4

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 35
• Clocking and Timing Overview, on page 37
• Configuring Clocking and Timing, on page 48
• Verifying the Configuration, on page 82
• Troubleshooting, on page 82
• Configuration Examples, on page 84

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.

The table below summarizes the PTP functionalities that are available, by license type:

<table>
<thead>
<tr>
<th>License</th>
<th>PTP Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metro Services</td>
<td>Not supported</td>
</tr>
<tr>
<td>Metro IP Service</td>
<td>Ordinary Slave Clock</td>
</tr>
<tr>
<td>Metro Aggregation Service</td>
<td>Ordinary Slave Clock</td>
</tr>
<tr>
<td>Metro IP Service + IEEE 1588-2008 BC/MC</td>
<td>All PTP functionality including boundary and master clock</td>
</tr>
<tr>
<td>Metro Aggregation Service + IEEE 1588-2008 BC/MC</td>
<td>All PTP functionality including boundary and master clock</td>
</tr>
</tbody>
</table>

**Note**

If you install the IEEE 1588-2008 BC/MC license, you must reload the chassis to use the full PTP functionality.

• 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

### 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 ASR 903 Series Aggregation Services Router 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 8: 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>
</tbody>
</table>
| Ordinary Clock (OC) | An ordinary clock is a 1588 clock with a single PTP port that can operate in one of the following modes:  
  • 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.  
  • 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. |
| Boundary Clock (BC) | The device participates in selecting the best master clock and can act as the master clock if no better clocks are detected. 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. |
**Network Element** | **Description**
--- | ---
Transparent Clock (TC) | 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.

---

**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 48.

Effective Cisco IOS-XE Release 3.18, the G.8275.1 telecom profile is also supported on the Cisco ASR 903 Series Routers 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 ASR 900 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 68.

**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 40) 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](image)

Table 9: 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 a OC master or BC master.
- Instead of each BC using same the 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 it’s 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.

![Diagram](image)

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 11: 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>
</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   |
### 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
```

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 68.

### 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 48 and Configuring a Boundary Clock, on page 56.
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

```
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

```
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 ASR 900 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 60.

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 ASR 900 Series Chassis does not currently support peer-to-peer transparent clock mode.

For information on how to configure the Cisco ASR 900 Series Chassis as a transparent clock, see Configuring a Transparent Clock, on page 58.

**Time of Day (TOD)**

You can use the time of day (ToD) and 1PPS ports on the Cisco ASR 900 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 ASR 900 Series Chassis, see the Configuring an Ordinary Clock, on page 48.

**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 73.

**Timing Port Specifications**

The following sections provide specifications for the timing ports on the Cisco ASR 900 Series Chassis.

**BITS Framing Support**

Table 12: Framing Modes for a BITS Port on a Cisco ASR 900 Series Chassis, on page 46 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 Chapter 1, “Configuring T1/E1 Interfaces.”

**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 75.

---

**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 80.
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 80.

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. `platform ptp master prte-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`
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 | linecode {ami | hdb3}}]
   • network-clock input-source priority external {R0 | R1} [120ohms | 75ohms | linecode {ami | hdb3}}]
   • 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><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> platform ptp master ptc-only-enable</td>
<td>(Optional) Enable Master port deletion.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# platform ptp master ptc-only-enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ptp clock {ordinary</td>
<td>boundary</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ptp clock ordinary domain 0</td>
<td>• ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ptp-clock)#</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.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong> priority1 priorityvalue</td>
<td>Sets the preference level for a clock. Slave devices use the priority1 value when selecting a master clock: a lower priority1 value indicates a preferred clock. The priority1 value is considered above all other clock attributes. Valid values are from 0-255. The default value is 128.</td>
</tr>
<tr>
<td><strong>Step 6</strong> priority2 priorityvalue</td>
<td>Sets a secondary preference level for a clock. Slave devices use the priority2 value when selecting a master clock: a lower priority2 value indicates a preferred clock. The priority2 value is considered only when the chassis is unable to use priority1 and other clock attributes to select a clock. Valid values are from 0-255. The default value is 128.</td>
</tr>
</tbody>
</table>
| **Step 7** utc-offset value leap-second “date time” offset [-1 | 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 8** input [1pps] {R0 | R1} | Enables Precision Time Protocol input 1PPS using a 1PPS input port. Use R0 or R1 to specify the active RSP slot. |
| **Step 9** tod {R0 | R1} {ubx | nmea | cisco | ntp} | Configures the time of day message format used by the ToD interface.  
  **Note** The ToD port acts as an input port in case of Master clock and as an output port in case of Slave clock. |
| **Step 10** clock-port port-name {master | slave} [profile {g8265.1}] | Defines a new clock port and sets the 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. |
<table>
<thead>
<tr>
<th>Step 11</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do one of the following:</td>
<td>Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.</td>
</tr>
<tr>
<td>• transport ipv4 unicast interface interface-type interface-number [negotiation]</td>
<td>The <strong>negotiation</strong> keyword configures the chassis to discover a PTP master clock from all available PTP clock sources.</td>
</tr>
<tr>
<td>• transport ethernet unicast [negotiation]</td>
<td>Note: PTP redundancy is supported only on unicast negotiation mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation
```

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits clock-port configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-clock synchronization automatic</td>
<td>Enables automatic selection of a clock source.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config)# network-clock synchronization automatic
```

<table>
<thead>
<tr>
<th>Step 14</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-clock synchronization mode ql-enabled</td>
<td>Enables automatic selection of a clock source based on quality level (QL).</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config)# network-clock synchronization mode ql-enabled
```

<table>
<thead>
<tr>
<th>Step 15</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use one of the following options:</td>
<td>• (Optional) To nominate SDH or SONET controller as network clock input source.</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>• network-clock input-source priority interface type/slot/port</td>
<td>• (Optional) To nominate Ethernet interface as network clock input source.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config)# network-clock input-source 1 external R0 10m
```

<table>
<thead>
<tr>
<th>Step 16</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock destination source-address</td>
<td>mac-address {bridge-domain bridge-domain-id}</td>
</tr>
</tbody>
</table>

**Example:**
```
clock destination 10.0.0.1
```

---

**Note:**
- Using a telecom profile requires that the clock have a domain number of 4–23.
- Specified the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.
- PTP redundancy is supported only on unicast negotiation mode.
- This command must be configured before any input source.
- This command is disabled by default.
### Configuring Clocking and Timing

#### Configuring a Master Ordinary Clock

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-ptp-port)# clock-source 8.8.8.1</code></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><strong>Step 17</strong></td>
<td></td>
</tr>
<tr>
<td><code>sync interval interval</code></td>
<td>Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
| `Router(config-ptp-port)# sync interval -4` | - 1—1 packet every 2 seconds  
- 0—1 packet every second  
- -1—1 packet every 1/2 second, or 2 packets per second  
- -2—1 packet every 1/4 second, or 4 packets per second  
- -3—1 packet every 1/8 second, or 8 packets per second  
- -4—1 packet every 1/16 seconds, or 16 packets per second.  
- -5—1 packet every 1/32 seconds, or 32 packets per second.  
- -6—1 packet every 1/64 seconds, or 64 packets per second.  
- -7—1 packet every 1/128 seconds, or 128 packets per second. |
| **Step 18**       |         |
| `announce interval interval` | Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows: |
| Example:          |         |
| `Router(config-ptp-port)# announce interval 2` | - 3—1 packet every 8 seconds  
- 2—1 packet every 4 seconds  
- 1—1 packet every 2 seconds  
- 0—1 packet every second  
- -1—1 packet every 1/2 second, or 2 packets per second  
- -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`             | Exit configuration mode. |
| Example:          |         |
| `Router(config-ptp-port)# end` |         |
| **Step 20**       |         |
| `linecode {ami | b8zs | hdb3}` | Selects the linecode type. |
| Example:          |         |
| `Router(config-controller)# linecode ami` | - ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers. |
Configuring Clocking and Timing

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>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: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ptp clock {ordinary</td>
<td>boundary</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<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>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
</tbody>
</table>
#### Configuring a Slave Ordinary Clock

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Router(config)# ptp clock ordinary domain 0 | • 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**

| output [1pps | R0 | R1] [offset offset-value] [pulse-width value] | Enables Precision Time Protocol input 1PPS using a 1PPS input port.  
Use R0 or R1 to specify the active RSP slot. |
|----------------|----------------|----------------------------------|
| Example:        | Router(config-tp-clock)# output 1pps R0 offset 200 pulse-width 20 μsec | Configures the time of day message format used by the ToD interface.  
*Note* Effective Cisco IOS XE Everest 16.6.1, on the Cisco ASR 900 RSP2 module, the 1pps pulse bandwidth can be changed from the default value of 500 milliseconds to up to 20 microseconds. |

**Step 5**

| tod | R0 | R1 | ubx | nmea | cisco | ntp | Configures the time of day message format used by the ToD interface.  
*Note* The ToD port acts as an input port in case of Master clock and as an output port in case of Slave clock. |
|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| Example:        | Router(config-tp-clock)# tod R0 ntp | 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 6**

| clock-port port-name master | slave | [profile {g8265.1}] | Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.  
The **negotiation** keyword 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. |
|-----------------------------|-------|---------------------|-----------------------------|
| Example:                    | Router(config-tp-clock)# clock-port Slave slave | Do one of the following:  
• transport ipv4 unicast interface interface-type interface-number [negotiation]  
• transport ethernet unicast [negotiation] |.Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.  
The **negotiation** keyword 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. |

---

**Cisco ASR 900 Router Series Configuration Guide, Cisco IOS XE Release 3S**

**OL-31439-01**
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>`clock source source-address</td>
<td>mac-address {bridge-domain bridge-domain-id}</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-ptp-port)# clock-source 8.8.8.1</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>announce timeout value</code></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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-ptp-port)# announce timeout 8</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>delay-req interval interval</code></td>
<td>Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state. The intervals are set using log base 2 values, as follows:</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
|      | `Router(config-ptp-port)# delay-req interval 1` | - 3—1 packet every 8 seconds  
- 2—1 packet every 4 seconds  
- 1—1 packet every 2 seconds  
- 0—1 packet every second  
- -1—1 packet every 1/2 second, or 2 packets per second  
- -2—1 packet every 1/4 second, or 4 packets per second  
- -3—1 packet every 1/8 second, or 8 packets per second  
- -4—1 packet every 1/16 seconds, or 16 packets per second.  
- -5—1 packet every 1/32 seconds, or 32 packets per second.  
- -6—1 packet every 1/64 seconds, or 64 packets per second.  
- -7—1 packet every 1/128 seconds, or 128 packets per second. |
| 11   | `end` | Exit configuration mode. |
|      | **Example:** | | |
|      | `Router(config-ptp-port)# end` | | |
| 12   | `Router(config-controller)# linecode \{ami | b8zs | hdb3\}` | Selects the linecode type. |
### Command or Action | Purpose
--- | ---
| • ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers. | **Purpose**
| • b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines. | **Purpose**
| • hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines. | **Purpose**

### 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>
</table>
| **Step 1** enable  
Example:  
Router> enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Step 2** configure terminal  
Example:  
Router# configure terminal | Enter configuration mode. |
| **Step 3** Router(config)# ptp clock {ordinary | boundary | e2e-transparent} domain domain-number [hybrid]  
Example: | Configures the PTP clock. You can create the following clock types:  
• ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode. |
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Router(config)# ptp clock boundary domain 0 | • 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

**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

**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 6

**transport ipv4 unicast interface interface-type interface-number [negotiation]**

**Example:**

Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 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.

**Note** PTP redundancy is supported only on unicast negotiation mode.

#### Step 7

**clock-source source-address [priority]**

**Example:**

Router(config-ptp-port)# clock source 133.133.133.133

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.
## Configuring Clocking and Timing

### Configuring a Transparent Clock

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

#### What to do next

### Configuring a Transparent Clock

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

#### What to do next

### Configuring a Transparent Clock

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

#### What to do next
The transparent clock ignores the domain number.

### 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></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Enter your password if prompted.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`ptp clock {ordinary</td>
<td>boundary</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>`Router(config)# ptp clock e2e-transparent</td>
<td></td>
</tr>
<tr>
<td><code>domain 4</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exit configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>`Router(config-controller)# linecode {ami</td>
<td>b8zs</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>· ami—Specifies Alternate Mark Inversion (AMI) as the linecode type.</td>
</tr>
<tr>
<td></td>
<td>· b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type.</td>
</tr>
<tr>
<td></td>
<td>· hdb3—Specifies high-density binary 3 (hdb3) as the linecode type.</td>
</tr>
</tbody>
</table>
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 \| hdb3\}\}\}`
   - `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\}`
<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>
<tr>
<td><strong>Step 4</strong> time-properties persist value</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>Example:</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>
<tr>
<td>Router(config-ptp-clk)# time-properties persist 600</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> utc-offset value leap-second &quot;date time&quot; offset {-1</td>
<td>1}</td>
</tr>
<tr>
<td>Example:</td>
<td>Valid values are from 0-255. The default value is 36.</td>
</tr>
<tr>
<td>Router(config-ptp-clk)# utc-offset 45 leap-second &quot;01-01-2017 00:00:00&quot; offset 1</td>
<td>(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.</td>
</tr>
<tr>
<td>• &quot;date time&quot;—Leap second effective date in dd-mm-yyyy hh:mm:ss format.</td>
<td>• boundary—Terminates PTP session from</td>
</tr>
<tr>
<td></td>
<td>Grandmaster and acts as PTP master to slaves downstream.</td>
</tr>
</tbody>
</table>
### Configuring Clocking and Timing

#### Configuring a Hybrid Boundary Clock

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>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.</strong>&lt;br&gt;<strong>Valid values are from 0-255.</strong></td>
</tr>
<tr>
<td><code>min-clock-class value</code></td>
<td><strong>Note</strong> Min-clock-class value is supported only for PTP with single master source configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-ptp-clk)# min-clock-class 157</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP master clock.</strong>&lt;br&gt;<strong>Note</strong> Hybrid mode is only supported with slave clock-ports; master mode is not supported.</td>
</tr>
<tr>
<td>`clock-port port-name {master</td>
<td>slave} [profile {g8265.1}]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-ptp-clk)# clock-port SLAVE slave</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>Specifies the transport mechanism for clocking traffic.</strong>&lt;br&gt;<strong>negotiation</strong>—(Optional) configures the chassis to discover a PTP master clock from all available PTP clock sources.</td>
</tr>
<tr>
<td><code>transport ipv4 unicast interface interface-type interface-number [negotiationsingle-hop]</code></td>
<td><strong>Note</strong> PTP redundancy is supported only on unicast negotiation mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-rtpt-port)# transport ipv4 unicast interface Loopback 0 negotiation or Router(config-rtpt-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>Specifies the address of a PTP master clock. You can specify a priority value as follows:</strong>&lt;br&gt;• No priority value—Assigns a priority value of 0.&lt;br&gt;• 1—Assigns a priority value of 1.&lt;br&gt;• 2—Assigns a priority value of 2, the highest priority.</td>
</tr>
<tr>
<td><code>clock-source source-address [priority]</code></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>Example:</strong></td>
<td>Router(config-rtpt-port)# clock source 133.133.133.133</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>Sets the clock port to PTP master or slave mode; in master mode, the port exchanges timing packets with PTP slave devices.</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td>`clock-port port-name {master</td>
<td>slave} [profile {g8265.1}]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-rtpt-port)# clock-port MASTER master</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 11</th>
<th>transport ipv4 unicast interface interface-type interface-number [negotiation] /single-hop</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-ptp-port)# transport ipv4 unicast interface Lo1 negotiation or Router(config-ptp-port)# transport ipv4 unicast interface Lo1 negotiation single-hop</td>
</tr>
</tbody>
</table>

**Purpose:** 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.

<table>
<thead>
<tr>
<th>Step 12</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Exit clock-port configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th>network-clock synchronization automatic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# network-clock synchronization automatic</td>
</tr>
</tbody>
</table>

**Purpose:** Enables automatic selection of a clock source.

**Note:** This command must be configured before any input source.

<table>
<thead>
<tr>
<th>Step 14</th>
<th>network-clock synchronization mode ql-enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# network-clock synchronization mode ql-enabled</td>
</tr>
</tbody>
</table>

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

**Note:** This command is disabled by default.

<table>
<thead>
<tr>
<th>Step 15</th>
<th>Use one of the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# network-clock input-source 1 external R0 10m</td>
</tr>
</tbody>
</table>

- **(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 Ethernet interface as network clock input source.

<table>
<thead>
<tr>
<th>Step 16</th>
<th>network-clock synchronization input-threshold ql value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# network-clock synchronization input-threshold &lt;ql value&gt;</td>
</tr>
</tbody>
</table>

**Purpose:** (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,
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>will be selected to recover the frequency. Otherwise, internal clock is selected.</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 17

**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 chassis 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 35

#### Step 18

**platformptpmasteralways-on**

**Example:**

Router(config)# platform ptp master always-on

(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.

#### Step 19

**platformptphybrid-bcdownstream-enable**

**Example:**

Router(config)# platform ptp hybrid-bc downstream-enable

(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.

#### Step 20

**end**

**Example:**

Router(config)# end

Exit configuration mode.

#### Step 21

**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 Hybrid Ordinary Clock

Follow these steps to configure a hybrid clocking in ordinary clock slave mode.
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 | 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. `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 ql-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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></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></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`ptp clock {ordinary</td>
<td>boundary</td>
</tr>
</tbody>
</table>
### Configuring a Hybrid Ordinary Clock

#### Command or Action

<table>
<thead>
<tr>
<th>Example:</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Router(config)# ptp clock ordinary domain 0 hybrid | • ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.  
  **Note** Hybrid mode is only supported with slave clock-ports; master mode is not supported.  
  • 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

| output {1pps} {R0 | R1} [offset offset-value] [pulse-width value] | Enables Precision Time Protocol input 1PPS using a 1PPS input port.  
  Use R0 or R1 to specify the active RSP slot.  
  **Note** Effective Cisco IOS XE Everest 16.6.1, on the Cisco ASR 900 RSP2 module, the 1pps pulse bandwidth can be changed from the default value of 500 milliseconds to up to 20 microseconds. |

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-tp-clk)# output 1pps R0 offset 200 pulse-width 20 μsec</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 5

| tod {R0 | R1} {ubx | nmea | cisco | ntp} | Configures the time of day message format used by the ToD interface.  
  **Note** The ToD port acts as an input port in case of Master clock and as an output port in case of Slave clock. |

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-tp-clk)# tod R0 ntp</td>
<td></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.  
  **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.  
  **Note** Using a telecom profile requires that the clock have a domain number of 4–23. |

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-tp-clk)# clock-port SLAVE slave</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 7

| transport ipv4 unicast interface interface-type interface-number [negotiation] | Specifies the transport mechanism for clocking traffic.  
  The **negotiation** keyword configures the router to discover a PTP master clock from all available PTP clock sources.  
  **Note** PTP redundancy is supported only on unicast negotiation mode. |

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-tp-port)# transport ipv4 unicast interface Loopback 0 negotiation</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 8** 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-pte-port)# clock source 133.133.133.133 | |
| **Step 9** exit | Exit clock-port configuration. |
| Example: Router(config-pte-port)# exit | |
| **Step 10** network-clock synchronization automatic | Enables automatic selection of a clock source.  |
| Example: Router(config-pte-clk)# network-clock synchronization automatic | Note: This command must be configured before any input source. |
| **Step 11** network-clock synchronization mode ql-enabled | Enables automatic selection of a clock source based on quality level (QL).  |
| Example: Router(config-pte-clk)# network-clock synchronization mode ql-enabled | Note: This command is disabled by default.  |
| For more information about this command, see Configuring Clocking and Timing, on page 35 | |
| **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}]  
  - 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> | (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 e1 mode.  
  - (Optional) To nominate BITS port as network clock input source in t1 mode.  
  - (Optional) To nominate Ethernet interface as network clock input source. |
| Example: Router(config)# network-clock input-source 1 external R0 10m | |
| **Step 13** network-clock hold-off {0 | milliseconds} | (Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a |
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>
</table>
| **Step 1**<br>enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:**
Router> enable |
| **Step 2**<br>configure terminal | Enter configuration mode. |
| **Example:**
Router# configure terminal |
| **Step 3**<br>ptp clock {ordinary | boundary | e2e-transparent} domain domain-number [hybrid] | Configures the PTP clock. You can create the following clock types:  
• 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. |
| **Example:**
Router(config)# ptp clock ordinary domain 0 |
| **Step 4**<br>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.  
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. |
| **Example:**
Router(config-ptp-clk)# clock-port SLAVE slave |
| **Step 5**<br>transport ipv4 unicast interface interface-type interface-number [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) It ensures that the PTP node communicates only with the adjacent nodes. |
| **Example:**
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation |
| **Step 6**<br>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. |
| **Example:**

### 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`

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config-ptp-port)# clock source 133.133.133.133 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> clock-source source-address [priority]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-ptp-port)# clock source 133.133.133.134 2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> clock-source source-address [priority]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-ptp-port)# clock source 133.133.133.135</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-ptp-port)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> linecode {ami</td>
<td>b8zs</td>
</tr>
<tr>
<td>Selects the linecode type.</td>
<td></td>
</tr>
<tr>
<td>• ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
</tbody>
</table>
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>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</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>
<tr>
<td>domain domain-number</td>
<td>• ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• boundary—Terminates PTP session from Grandmaster and acts as PTP master to slaves downstream.</td>
</tr>
<tr>
<td>Router(config)# ptp clock boundary domain 0</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>Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP master clock.</td>
</tr>
<tr>
<td>clock-port port-name {master</td>
<td>slave} [profile {g8265.1}]</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>Note</strong> Using a telecom profile requires that the clock have a domain number of 4–23.</td>
</tr>
<tr>
<td>Router(config-ptp-clk)# clock-port SLAVE slave</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies the transport mechanism for clocking traffic.</td>
</tr>
<tr>
<td>transport ipv4 unicast interface interface-type interface-number [negotiation] /single-hop</td>
<td>• <strong>negotiation</strong>—(Optional) Configures the chassis to discover a PTP master clock from all available PTP clock sources.</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>Note</strong> PTP redundancy is supported only on unicast negotiation mode.</td>
</tr>
<tr>
<td>Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation</td>
<td>• <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>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring PTP Redundancy in Boundary Clock Mode

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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. |
| **Step 9**
- **clock-port** port-name {master | slave} [profile {g8265.1}]
  Example:
  ```
  Router(config-ptp-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-ptp-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.
  - **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.
  **Note** PTP redundancy is supported only on unicast negotiation mode. |
| **Step 11**
- **end**
  Example:
  ```
  Router(config-ptp-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. |
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
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 48. 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>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></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</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>
</tbody>
</table>
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 53.

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><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></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}}}]
   - network-clock input-source priority external {R0 | R1} {2048k | e1 {crc4 | fas} {120ohms | 75ohms} {linecode {ami | hdb3}}

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| Step 3 tod-clock input-source priority {gps | In slave mode, specify a PTP domain as a ToD input source.  
                                           | R0 | R1} | ptp  |
                                           | domain | domain |                                               |
                                           | Example:                                      |.Router(config)# TOD-clock 10 ptp domain 0       |
                                           | Step 4 Router(config)# end                   | Exit configuration mode.                      |
                                           | Step 5 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 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.  
                                           |                                           |                                               |
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>network-clock synchronization automatic</code></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Note</strong> This command must be configured before any input source.</td>
</tr>
<tr>
<td><code>Router(config)# network-clock synchronization automatic</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>`network-clock eec {1</td>
<td>2}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• 1—ITU-T G.8262 option 1 (2048)</td>
</tr>
<tr>
<td><code>Router(config)# network-clock eec 1</code></td>
<td>• 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544)</td>
</tr>
</tbody>
</table>

#### Examples
- **Step 1**: `Router> enable`
- **Step 2**: `Router# configure terminal`
- **Step 3**: `Router(config)# network-clock synchronization automatic`
- **Step 4**: `Router(config)# network-clock eec 1`
### Command or Action

**Step 5**

`network-clock synchronization ssm option {1 | 2 | GEN1 | GEN2}`

**Example:**

Router(config)# network-clock synchronization ssm option 2 GEN2

**Purpose**

Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command:

- Option 1 refers to G.781 synchronization option 1, which is designed for Europe. This is the default value.
- 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.

**Step 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}`
- `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`

**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 e1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.
- (Optional) To nominate PTP as network clock input source.

**Step 7**

`network-clock synchronization mode ql-enabled`

**Example:**

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

**Purpose**

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

**Purpose**

(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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong> network-clock wait-to-restore <em>seconds</em></td>
<td>(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. <strong>Note</strong> You can also specify a wait-to-restore value for an individual interface using the network-clock wait-to-restore command in interface mode.</td>
</tr>
</tbody>
</table>
| **Example:** \[
\text{Router(config)# network-clock wait-to-restore 70}
\] |
| **Step 10** 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. |
| **Example:** \[
\text{Router(config)# network-clock revertive}
\] |
| **Step 11** esmc process | Enables the ESMC process globally. |
| **Example:** \[
\text{Router(config)# esmc process}
\] |
| **Step 12** network-clock external *slot/card/port* hold-off \{0 | milliseconds\} | Overrides the hold-off timer value for the external interface. |
| **Example:** \[
\text{Router(config)# network-clock external 0/1/0 hold-off 0}
\] |
| **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: 1. **Option 1**—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU. 2. **Option 2**, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS. 3. **Option 2**, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS. |
| **Example:** \[
\text{Router(config)# network-clock quality-level rx qL-pRC external R0 e1 cas crc4}
\] |
| **Step 14** interface *type number* | Enters interface configuration mode. |
| **Example:** \[
\text{Router(config)# interface GigabitEthernet 0/0/1}
\] |
### Command or Action

| Step 15 | synchronous mode  
Example:  
Router(config-if)# synchronous mode | Configure the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface. |
|---------|----------------------------------------------------------|
| Step 16 | network-clock source quality-level value {tx | rx}  
Example:  
Router(config-if)# network-clock source quality-level QL-PrC tx | 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:  
- Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.  
- Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.  
- Option 2, GEN2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS. |
| Step 17 | esmc mode [ql-disabled | tx | rx] value  
Example:  
Router(config-if)# esmc mode rx QL-STU | Enables the ESMC process at the interface level. The `no` form of the command disables the ESMC process. |
| Step 18 | network-clock hold-off {0 | milliseconds}  
Example:  
Router(config-if)# network-clock hold-off 0 | (Optional) Configures an interface-specific hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.  
You can configure the hold-off time to either 0 or any value between 50 to 10000 ms. The default value is 300 ms. |
| Step 19 | network-clock wait-to-restore seconds  
Example:  
Router(config-if)# network-clock wait-to-restore 70 | (Optional) Configures the wait-to-restore timer for an individual synchronous Ethernet interface. |
| Step 20 | end  
Example:  
Router(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |

### What to do next

You can use the `show network-clocks` command to verify your configuration.
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.

The new clock source must be of higher quality than the current clock source; otherwise the chassis does not select the new 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.

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

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>
</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 R0</td>
</tr>
</tbody>
</table>

Disabling a Clock Source

To disable a clock source selection, 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>Router# network-clock clear switch t0</td>
<td></td>
</tr>
</tbody>
</table>

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 R0</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>Router# network-clock clear switch t0</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Clocking and Timing

#### 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.
- `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 13: SyncE Debug Commands** on page 82 list the debug commands that are available for troubleshooting the SyncE configuration on the chassis:

<table>
<thead>
<tr>
<th>Debug Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug platform network-clock</code></td>
<td>Debugs issues related to the network clock including active-standby selection, alarms, and OOR messages.</td>
</tr>
<tr>
<td><code>debug network-clock</code></td>
<td>Debugs issues related to network clock selection.</td>
</tr>
</tbody>
</table>

We recommend that you do not use debug commands without TAC supervision.
### Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug esmc error</code></td>
<td>These commands verify whether the ESMC packets are transmitted and received with proper quality-level values.</td>
</tr>
<tr>
<td><code>debug esmc event</code></td>
<td></td>
</tr>
<tr>
<td><code>debug esmc packet [interface interface-name]</code></td>
<td></td>
</tr>
<tr>
<td><code>debug esmc packet rx [interface interface-name]</code></td>
<td></td>
</tr>
<tr>
<td><code>debug esmc packet tx [interface interface-name]</code></td>
<td></td>
</tr>
</tbody>
</table>

### Table 14: Troubleshooting Scenarios

<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` 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. |
| **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` command.  
   • Use the `show network-clock synchronization` command to confirm if the system is in revertive mode or nonrevertive 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` 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. |
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

```plaintext
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)

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

Ordinary Clock—Master

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

Ordinary Clock—Master (Ethernet)

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

Unicast Configuration—Slave Mode

```plaintext
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)**

```plaintext
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**

```plaintext
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)**

```plaintext
ptp clock ordinary domain 0
clock-port Master master
transport ethernet unicast
clock destination 1234.5678.90ab bridge-domain 5
```

**Unicast Negotiation—Slave**

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

**Unicast Negotiation—Slave (Ethernet)**

```plaintext
ptp clock ordinary domain 0
clock-port Slave slave
transport ethernet unicast negotiation
clock source 1234.5678.90ab bridge-domain 5 5
clock-port Slave1 slave
transport ethernet unicast negotiation
clock source 1234.9876.90ab interface gigabitethernet 0/0/4 2
```

**Unicast Negotiation—Master**

```plaintext
ptp clock ordinary domain 0
clock-port Master master
transport ipv4 unicast interface loopback 0 negotiation
sync interval 1
announce interval 2
```

**Unicast Negotiation—Master (Ethernet)**

```plaintext
ptp clock ordinary domain 0
clock-port Master master
transport ethernet unicast negotiation
```
**Boundary Clock**

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

**Transparent Clock**

`ptp clock e2e-transparent domain 0`

**Hybrid Clock—Boundary**

`ptp clock boundary domain 0 hybrid`  
`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`  
  `clock source 5.5.5.5 1`  
  `clock source 5.5.5.5 2`

**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`  
  `clock source 5.5.5.5 1`  
  `clock source 5.5.5.5 2`  
`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 33.1.1.1

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
PTP Ordinary Clock [Domain 0]

<table>
<thead>
<tr>
<th>State</th>
<th>Ports</th>
<th>Pkts sent</th>
<th>Pkts rcvd</th>
<th>Redundancy Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACQUIRING</td>
<td>1</td>
<td>98405</td>
<td>296399</td>
<td>Track one</td>
</tr>
</tbody>
</table>

PORT SUMMARY

PTP Master

<table>
<thead>
<tr>
<th>Name</th>
<th>Tx Mode</th>
<th>Role</th>
<th>Transport</th>
<th>State</th>
<th>Sessions</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLAVE</td>
<td>unicast</td>
<td>slave</td>
<td>Lo0</td>
<td>Slave</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

8.8.8.8

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

!output omitted for brevity

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]

---

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 Info for 0/0

---

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

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

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 Info for 0/0

---------------------------------------------------
ToD 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
SLAVE unicast slave Ethernet 1
9.9.9.1
MASTER unicast master Ethernet - 2 -

SESSION INFORMATION
SLAVE [Ethernet] [Sessions 1]
Peer addr Pkts in Pkts out In Errs Out Errs
9.9.9.1 159083 31054 0 0

MASTER [Ethernet] [Sessions 2]
Peer addr Pkts in Pkts out In Errs Out Errs
aabb.ccdd.ee01 [Gig0/2/3] 223 667 0 0
aabb.ccdd.ee02 [BD 1000] 210 634 0 0

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 gigabitehternet 0/0
  network-clock input-source 2 gigabitehternet 0/1
  network-clock synchronization mode QL-enabled
no network-clock revertive
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.

Effective Cisco IOS-XE Release 3.18S, Cisco ASR 903 routers with RSP2 module support the G.8275.1 telecom profile. This profile targets accurate time and phase distribution and requires boundary clocks at every node in the network.

Effective Cisco IOS-XE Release 3.18SP, Cisco ASR 903 routers with RSP3 module support the G.8275.1 telecom profile and G.8273.2 telecom recommendation.

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 91
- Configuring the G.8275.1 Profile, on page 96
- Additional References, on page 99
- Feature Information for G.8275.1, on page 100

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 4: 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.

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

Figure 5: Ordinary Clock As T-GM

1. OC that can only be a slave clock (T-TSC). In this case, only one PTP port is used for T-TSC, which in turn will have only one PTP master associated with it.
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.

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.

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.
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.
- When the Cisco ASR900 routers with RSP2 or RSP3 modules are configured with G.8275.1 Hybrid Boundary clock (T-BC) or Hybrid Slave clock (T-TSC), the combination of PTP and SyncE drives all timing outputs except BITS. This implies that clock outputs are compliant to G.8273.2 and track the Hybrid PTP clock. BITS output always tracks only to the input electrical clock and is not influenced by PTP.
- Virtual port is not supported on the Cisco RSP2 Module.
Configuring the G.8275.1 Profile

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
```

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
```

Creating Dynamic Ports

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

```
ptp clock boundary domain 24 hybrid
```
G.8275.1 Telecom Profile

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 R0ntp
```

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
  Slave Only: No
  Clock Quality:
    Class: 224
    Accuracy: Unknown
    Offset (log variance): 4252
```

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
```
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.
The configuration on master clock A is:

```plaintext
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:

```plaintext
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:

```plaintext
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:

```plaintext
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>
</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 101 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>
<tbody>
<tr>
<td>G.8275.1 Support for 1588 profile</td>
<td>XE 3.18</td>
<td>This PTP telecom profile introduces phase and time synchronization with full timing support from the network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>local-priority</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were modified:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>clock-port</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>show ptp clock dataset default</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>show ptp port dataset port</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following command is deprecated for the G.8275.1 profile clocks:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>show ptp port running</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The alternate command is <code>show platform software ptp foreign-master [domain-number]</code>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td>This command is applicable only for the G.8275.1 profile clocks.</td>
</tr>
</tbody>
</table>
CHAPTER 6

Configuring the Global Navigation Satellite System

Effective Cisco IOS-XE Release 3.17, the Cisco ASR 903 (with RSP3 module) and Cisco ASR 907 router 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 103
- How to Configure the GNSS, on page 105
- Configuration Example For Configuring GNSS, on page 108
- Additional References, on page 108

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 its 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 its 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.

**High Availability for GNSS**

The Cisco ASR 903 and Cisco ASR 907 routers have 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 in the *Cisco ASR 903 Router Chassis Software Configuration Guide*.
- 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 ASR 903 Series Aggregation Services Router 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**

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>To know more about the commands referenced in this document, see the <em>Cisco IOS Master Command List</em>.</td>
</tr>
</tbody>
</table>

**Enabling the GNSS on the Cisco Router**

```bash
enable
cfg-term
gnss slot r0
no shutdown
exit
```

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>After the GNSS module is enabled, GNSS will be the source for 1PPS, ToD, and 10MHz clocking functions.</td>
</tr>
</tbody>
</table>

**Configuring the Satellite Constellation for GNSS**

```bash
enable
cfg-term
```
Configuring Pulse Polarity

```
enable
configure terminal
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
configure terminal
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
configure terminal
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.

```bash
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>47</td>
</tr>
<tr>
<td>27</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>44</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>
```

```bash
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
```

Use the `show gnss time` and `show gnss location` to display the time and location of the Cisco ASR 902 or Cisco ASR907 router.

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

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

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

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

Use the `show gnss device` to display the hardware information of the active GNSS module.

```bash
Router# show gnss device
GNSS device:

Serial number: FOC2130ND5X
Firmware version: 1.4
Firmware update progress: NA
Authentication: Passed
```
Configuration Example For Configuring GNSS

gnss slot R0
no shutdown
anti-jam disable
constellation 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: <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 associated RFCs for this feature.</td>
</tr>
</tbody>
</table>
CHAPTER 7

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 109
- Verifying the Interface Configuration, on page 121
- Verifying Interface Module Status, on page 122
- Configuring LAN/WAN-PHY Controllers, on page 123
- Configuration Examples, on page 130

Limitations and Restrictions

- VRF-Aware Software Infrastructure (VASI) interface commands interface vasileft and interface vasiright are not supported starting Cisco IOS XE Release 3.15.

- Interface modules have slot restrictions, see ASR 900 Series Hardware Installation Guides

- MPLS MTU is not supported on releases prior to Cisco IOS XE Release 3.10.2 on the router. This is not applicable for Cisco IOS XE Everest 16.5.1.

- IP MTU and MPLS MTU are supported. But MPLS MTU support is restricted only to CPU originated traffic. For the forwarded traffic, it is the IP MTU that decides the behavior.

- 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.

- Only A900-IMA8Z Interface Modules support LAN/WAN-PHY mode on the Cisco ASR 900 RSP3 Module.

- SNMP support is not available for WAN-PHY in Cisco IOS XE Release 3.18.1SP.
- IEEE 1588 and SyncE are not supported in the WAN-PHY mode on A900-IMA8Z Interface Modules.
- 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.

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

#### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> speed {10</td>
<td>100</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
**Router(config-if)# speed 1000** |
| **Step 6** mtu bytes | (As Required) Specifies the maximum packet size for an interface, where: |
| Example: | | 
**Router(config-if)# mtu 1500** |
| **Step 7** standby \[group-number\] ip \[ip-address [secondary]\] | Creates or enables the Hot Standby Router Protocol (HSRP) group using its number and virtual IP address, where: |
| Example: | | 
**Router(config-if)# standby 250 ip 192.168.10.1** |
| **Step 8** no shutdown | Enables the interface. |
| Example: | | 
**Router(config-if)# no shutdown** |

## 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.
The interface module slot number is always 0.

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

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

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

Configuring Hot Standby Router Protocol

Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts without relying on the availability of any single router. You can deploy HSRP in a group of routers to select an active router and a standby router. (An active router is the router of choice for routing packets; a standby router is a router that takes over the routing duties when an active router fails, or when preset conditions are met). HSRP is enabled on an interface by entering the `standby [group-number] ip [ip-address [secondary]]` command. The `standby` command is also used to configure various HSRP elements. This document does not discuss more complex HSRP configurations. For additional information on configuring HSRP, see to the HSRP section of the Cisco IP Configuration Guide publication that corresponds to your Cisco IOS XE software release. In the following HSRP configuration, standby group 2 on Gigabit Ethernet port 0/1/0 is configured at a priority of 110 and is also configured to have a preemptive delay should a switchover to this port occur:

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

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

The maximum number of HSRP or VRRP groups allowed are:

• RSP1A — 128 HSRP or VRRP groups. 128 HSRP or VRRP groups restriction implies that the maximum number of different interfaces that can be configured with VRRP or HSRP is 128. You cannot configure HSRP or VRRP for more than 128 interfaces but you can configure up to 256 HSRP or VRRP groups in those 128 interfaces.
• RSP1B — 256 HSRP or VRRP groups
• RSP2A-64 and RSP2-128 — 128 HSRP or VRRP groups, prior to Cisco IOS Release XE 3.15S
• RSP2A-64 and RSP2-128 — 256 HSRP or VRRP groups, starting Cisco IOS Release XE 3.15S
• RSP3-200 and RSP3-400 — 255 HSRP or VRRP groups, starting Cisco IOS Release XE 3.18.1SP
Verifying HSRP

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
Hellotime 3 holdtime 10
Next hello sent in 0:00:00
Hot standby IP address is 198.92.72.29 configured
Active router is local
Standby router is 198.92.72.21 expires in 0:00:07
Standby virtual mac address is 0000.0c07.ac00
Tracking interface states for 2 interfaces, 2 up:
UpSerial0
UpSerial1
```

Modifying the Interface MTU Size

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.

- **IP MTU**—Can be specified on an interface. If an IP packet exceeds the IP MTU size, then the packet is fragmented.

When the value of the IP MTU is 9216 bytes and the packet is sent with 9214 bytes, 18 bytes are added to the packet by FPGA. The total size of the packet then becomes 9232 bytes. The maximum supported MTU of the packet without fragmentation in ASIC is 9232, so there is no traffic loss with a packet size of 9214. When IP MTU is 9216, and the packet is sent with either 9215 or 9216 bytes, 18 bytes are added to the packet by FPGA. The total size of the packet then becomes 9233 or 9234 bytes respectively. As
the packet size exceeds the maximum supported MTU size of the packet without fragmentation, the packet is dropped.

When the traffic with packet size greater than 9216 bytes is sent and the MTU is configured as 9216 bytes, the packet is fragmented. Hence, the packet loss is prevented.

Note
The IP MTU configured on BDI should not be greater than the Layer2 MTU configured on the underlying Layer2 interface. For Cisco ASR 900 RSP3 Module the IP MTU configured on a BDI should be equal to the Layer2 MTU configured on the underlying Layer 2 interface.

- 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.

Encapsulation methods and MPLS MTU labels add additional overhead to a packet. For example, Subnetwork Access Protocol (SNAP) encapsulation adds an 8-byte header, dot1q encapsulation adds a 2-byte header, and each MPLS label adds a 4-byte header (n labels x 4 bytes).

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

Note
If you are using MPLS, ensure that the mpls mtu command is configured for a value less than or equal to the interface MTU. This is not applicable for Cisco ASR 900 RSP3 Module.

- If you are using MPLS labels, then you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.
• 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>
<tbody>
<tr>
<td>mtu bytes</td>
<td>Configures the maximum packet size for an interface, where:</td>
</tr>
<tr>
<td></td>
<td>• bytes—Specifies the maximum number of bytes for a packet.</td>
</tr>
<tr>
<td></td>
<td>The default is 1500 bytes and the maximum configurable MTU is 9216 bytes.</td>
</tr>
</tbody>
</table>

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 A900-IMA8T , address is d0c2.8216.0590 (bia d0c2.8216.0590)
  MTU 1500 bytes
  , BW 1000000 Kbit/sec, DLY 10 usec,
  , reliability 255/255, txload 1/255, rxload 22/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)

MPLS MTU

MPLS MTU configuration is supported starting with Cisco IOS XE Release 3.10.2 and later. The platform mpls mtu-enable command is introduced to enable MPLS MTU on the router.
Restrictions

- MPLS MTU is not supported if IP address is not configured on the interface.
- MPLS MTU is not supported with MPLS LDP Auto configuration.
- MPLS MTU is not supported with BGP send-label.
- IP MTU configuration on an interface does not program MPLS MTU in the hardware. MPLS MTU value is obtained from the Interface MTU or IP MTU.
- In releases prior to Cisco IOS XE Release 3.10.2, if IP MTU is changed, MPLS MTU also changes.
- If both Interface MTU and IP MTU are configured MPLS MTU is obtained from IP MTU. See Table 16: MTU Normal Behavior (Command Not Enabled), on page 117.

Table 16: MTU Normal Behavior (Command Not Enabled)

<table>
<thead>
<tr>
<th>Interface-MTU</th>
<th>IP MTU</th>
<th>MPLS MTU</th>
<th>MPLS MTU Value Derived</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Interface MTU</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>IP MTU</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>IP MTU</td>
</tr>
</tbody>
</table>

- If MPLS MTU is enabled using `platform mpls mtu-enable` command, then IP MTU does not affect the MPLS MTU configuration. See Table 17: MTU Behavior with platform mpls mtu-enable Command Configured, on page 117.

Table 17: MTU Behavior with platform mpls mtu-enable Command Configured

<table>
<thead>
<tr>
<th>Interface MTU</th>
<th>IP MTU</th>
<th>MPLS MTU</th>
<th>MPLS MTU Value Derived</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Interface MTU</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Default value</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Interface MTU</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Default value</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>MPLS MTU</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>MPLS MTU</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>MPLS MTU</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>MPLS MTU</td>
</tr>
</tbody>
</table>

Configuring MPLS MTU Globally

We recommend not to toggle the command as inconsistent results may be displayed.
After configuring or unconfiguring the command, we recommend that all MTU values on all the interfaces are re-configured.

SUMMARY STEPS

1. `platform mpls mtu-enable`
2. `interface gigabitethernet slot /subslot /port`
3. `mpls mtu mtu-value`

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><code>platform mpls mtu-enable</code></td>
<td>Configures MPLS MTU globally on the router</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router (config)# platform mpls mtu-enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface gigabitethernet slot /subslot /port</code></td>
<td>Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router (config)# interface GigabitEthernet 0/0/1</code></td>
<td>Note The slot number is always 0.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>mpls mtu mtu-value</code></td>
<td>Configures the MTU value.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# mpls mtu 700</code></td>
<td></td>
</tr>
</tbody>
</table>

Verifying MPLS MTU

Use the `show platform hardware pp active feature mpls mtu-table` command to display the MPLS MTU values configured on the router.

```
Router# show platform hardware pp active feature mpls mtu-table
MPLS MTU Table
Index    MTU   Ref-Count
-----------------------------
 0       1504   1
 1       704    0
 2       0      0
 3       0      0
 4       0      0
 5       0      0
```
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.

For more information about how to configure these features, see the Configuring Ethernet Virtual Connections on the Cisco ASR 900 Series Router document.

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.

The Copper SFP does not auto-negotiate full duplex with 8-port Gigabit Ethernet RJ45 (Copper) Interface Module (8X1GE) with speed 100 configured.

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</td>
</tr>
<tr>
<td></td>
<td>interface. Advertisement of flow control occurs.</td>
</tr>
</tbody>
</table>

Router(config-if)# negotiation auto
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>

Router(config-if)# no negotiation auto

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 Configuration.

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>

Router# copy running-config startup-config

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.
### Shutting Down and Restarting an Interface Module

You can use the following commands in EXEC mode to automatically stop traffic on the affected interfaces and deactivate them along with the interface module in preparation for OIR:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>shutdown</strong></td>
<td>Restarts, stops, or starts an interface.</td>
</tr>
</tbody>
</table>

```
router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)
router(config)# interface GigabitEthernet 0/1/0
router(config-if)# shutdown
```

```
no shutdown
```

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

### 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 A900-IMA8T, 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 (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 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out

Verifying Interface Module Status

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

Note

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

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show hw-module slot/subslot transceiver port idprom</td>
<td>Displays information for the transceiver identification programmable read only memory (idprom).</td>
</tr>
<tr>
<td>Note</td>
<td>Transceiver types must match for a connection between two interfaces to become active.</td>
</tr>
<tr>
<td>show hw-module slot/subslot transceiver port idprom status</td>
<td>Displays information for the transceiver initialization status.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td>show hw-module slot/subslot transceiver port idprom dump</td>
<td>Displays a dump of all EEPROM content stored in the transceiver.</td>
</tr>
</tbody>
</table>

The following show hw-module subslot command sample output is for 1000BASE BX10-U:
Router#show hw-module subslot 0/2 transceiver 0 idprom brief

IDPROM for transceiver GigabitEthernet0/2/0:
- Description: SFP or SFP+ optics (type 3)
- Transceiver Type: 1000BASE BX10-U (259)
- Product Identifier (PID): GLC-BX-U
- Vendor Revision: 1.0
- Serial Number (SN): NPH20441771
- Vendor Name: CISCO-NEO
- Vendor OUI (IEEE company ID): 00.15.06 (5382)
- CLEI code: IPUIAG5RAC
- Cisco part number: 10-2094-03
- Device State: Enabled.
- Date code (yy/mm/dd): 16/11/12
- Connector type: LC.
- Encoding: 8B10B (1)
- Nominal bitrate: GE (1300 Mbits/s)
- Minimum bit rate as % of nominal bit rate: not specified
- Maximum bit rate as % of nominal bit rate: not specified

Router#

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

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

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

Router#

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 on the Cisco ASR 900 RSP3 Module.
- The following A900-IMA8Z IM alarms are not supported on the Cisco ASR 900 RSP3 Module:
  - NEWPTR
  - PSE
  - NSE
  - FELCDP
  - FEAISP

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 one of the following:
   - `hw-module subslot slot/subslot enable LAN`
   - `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></td>
<td><code>show controllers wanphy slot/subslot/port</code></td>
<td>Displays the configuration mode of the LAN/WAN-PHY controller. Default configuration mode is LAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# show controllers wanphy 0/1/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TenGigabitEthernet0/1/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Mode of Operation: WAN Mode</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECTION</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOF = 0</td>
<td>LOS = 0</td>
</tr>
<tr>
<td></td>
<td>BIP(B1) = 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LINE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIS = 0</td>
<td>RDI = 0</td>
</tr>
<tr>
<td></td>
<td>BIP(B2) = 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PATH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIS = 0</td>
<td>RDI = 0</td>
</tr>
<tr>
<td></td>
<td>BIP(B3) = 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOP = 0</td>
<td>NEWPTR = 0</td>
</tr>
<tr>
<td></td>
<td>NSE = 0</td>
<td>PSE = 0</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIS ALARMS SER = 0 FELCDP = 0 FEAISP = 0 WLOS = 0 PLCD = 0 LFEBIP = 0 PBEC = 0</td>
<td></td>
</tr>
<tr>
<td>Active Alarms [All defects]: SWLOF LAIS PAIS SER</td>
<td></td>
</tr>
<tr>
<td>Active Alarms [Highest Alarms]: SWLOF</td>
<td></td>
</tr>
<tr>
<td>Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA PLOP WLOS</td>
<td></td>
</tr>
<tr>
<td>Rx(K1/K2): 00/00 Tx(K1/K2): 00/00</td>
<td></td>
</tr>
<tr>
<td>S1S0 = 00, C2 = 0x1A PATH TRACE BUFFER: UNSTABLE</td>
<td></td>
</tr>
<tr>
<td>Remote J1 Byte : BER thresholds: SD = 10e-6 SF = 10e-3 TCA thresholds: B1 = 10e-6</td>
<td></td>
</tr>
<tr>
<td>B2 = 10e-6 B3 = 10e-6</td>
<td></td>
</tr>
</tbody>
</table>

### Step 2

**configure terminal**

**Example:**

```
Router# configure terminal
```

Enters global configuration mode.

### Step 3

**Do one of the following:**

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

**Example:**

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

Configures LAN-PHY mode for the Ethernet interface module.

**hw-module subslot slot/subslot enable LAN** command is only applicable for A900-IMA1X on the ASR 903 RSP1 and RSP2 Modules.

Use the `hw-module subslot slot/subslot interface port enable LAN` command to configure the LAN-PHY mode for the Ethernet interface module on the ASR 903 RSP3 Module.

**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
```

Displays configuration mode for the LAN/WAN-PHY controller. The example shows the mode of operation as LAN mode for the Cisco 8-Port 10 Gigabit Ethernet LAN/WAN-PHY Controller.

## Configuring WAN-PHY Mode

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

1. `show controllers wanphy slot/subslot/port`
2. `configure terminal`
3. Do one of the following:
   - `hw-module subslot slot/subslot enable WAN`
   - `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></td>
<td><code>show controllers wanphy slot/subslot/port</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Displays the configuration mode of the WAN-PHY controller. Default configuration mode is LAN.</td>
</tr>
<tr>
<td></td>
<td>- <code>slot/subslot /port</code> — The location of the interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <code>hw-module subslot slot/subslot enable WAN</code></td>
</tr>
<tr>
<td></td>
<td>- <code>hw-module subslot slot/subslot interface port enable WAN</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures WAN-PHY mode for the Ethernet interface module.</td>
</tr>
<tr>
<td></td>
<td>- <code>slot/subslot /port</code> — The location of the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Exits global configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show controllers wanphy slot/subslot/port</code></td>
</tr>
<tr>
<td>Example:</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>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Mode of Operation: WAN Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECTION</td>
</tr>
<tr>
<td>LOF = 0</td>
</tr>
<tr>
<td>LOS = 0</td>
</tr>
<tr>
<td>BIP(B1) = 0</td>
</tr>
<tr>
<td>LINE</td>
</tr>
<tr>
<td>AIS = 0</td>
</tr>
<tr>
<td>RDI = 0</td>
</tr>
<tr>
<td>FEBE = 0</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>BIP(B2) = 0</td>
</tr>
<tr>
<td>PATH</td>
</tr>
<tr>
<td>AIS = 0</td>
</tr>
<tr>
<td>RDI = 0</td>
</tr>
<tr>
<td>FEBE = 0</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>BIP(B3) = 0</td>
</tr>
<tr>
<td>LOP = 0</td>
</tr>
<tr>
<td>NEWPTR = 0</td>
</tr>
<tr>
<td>PSE = 0</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>NSE = 0</td>
</tr>
<tr>
<td>WIS ALARMS</td>
</tr>
<tr>
<td>SER = 0</td>
</tr>
<tr>
<td>FELCDP = 0</td>
</tr>
<tr>
<td>FEAISP = 0</td>
</tr>
<tr>
<td>= 0</td>
</tr>
<tr>
<td>WLOS = 0</td>
</tr>
<tr>
<td>PLCD = 0</td>
</tr>
<tr>
<td>LFEBIP = 0</td>
</tr>
<tr>
<td>PBEC = 0</td>
</tr>
<tr>
<td>Active Alarms[All defects]: SWLOF LAIS PAIS SER</td>
</tr>
<tr>
<td>Active Alarms[Highest Alarms]: SWLOF</td>
</tr>
<tr>
<td>Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA</td>
</tr>
<tr>
<td>PLOP WLOS</td>
</tr>
<tr>
<td>Rx(K1/K2): 00/00</td>
</tr>
<tr>
<td>Tx(K1/K2): 00/00</td>
</tr>
<tr>
<td>S1S0 = 0, C2 = 0x1A</td>
</tr>
<tr>
<td>PATH TRACE BUFFER: UNSTABLE</td>
</tr>
<tr>
<td>Remote J1 Byte:</td>
</tr>
<tr>
<td>BER thresholds: SD = 10e-6 SF = 10e-3</td>
</tr>
<tr>
<td>TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6</td>
</tr>
</tbody>
</table>

### Configuring the Flag for Path Trace

The 1-Port 10GE LAN/WAN-PHY Shared Port Adapter can operate in either the WAN mode or the LAN mode. To check end-to-end connectivity, J1 flag byte values can be configured on the local SPA. The configured J1 byte values are displayed at the remote end in the `show controllers wanphy interface-path-id` command output.

### SUMMARY STEPS

1. configure terminal
2. controller wanphy `interface-path-id`
3. wanphy flag j1 transmit `string`
4. exit
5. exit
6. show controller wanphy `<interface-path-id>`

### 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 the global configuration mode.</td>
</tr>
</tbody>
</table>
| Example:  
  Router# configure terminal | |

---

Cisco ASR 900 Router Series Configuration Guide, Cisco IOS XE Release 3S

OL-31439-01
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>controller wanphy interface-path-id</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# controller wanphy 2/1/0</td>
</tr>
<tr>
<td></td>
<td>Enters the controller mode of the WAN-PHY SPA. In this example, it enters slot 1 of SIP 2.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>wanphy flag j1 transmit string</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# wanphy flag j1 transmit passing_string_from_localend</td>
</tr>
<tr>
<td></td>
<td>Passes the string of J1 bytes specified to the remote end of WAN-PHY SPA. In this example, the string value passing_string_from_localend is transmitted to the remotely connected WAN-PHY SPA.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# exit</td>
</tr>
<tr>
<td></td>
<td>Exits Controller-configuration (config) mode and enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# exit</td>
</tr>
<tr>
<td></td>
<td>Exits global-configuration (config) mode and enters privilege-exec mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show controller wanphy &lt;interface-path-id&gt;</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# show controller wanphy 2/2/0 TenGigabitEthernet0/2/0 Mode of Operation: WAN Mode SECTION [LOF = 0 \ LOS = 0 \ BIP(B1) = 0 \ LINE \ AIS = 0 \ RDI = 0 \ FEBE = 0 \ BIP(B2) = 0 \ PATH \ AIS = 0 \ RDI = 0 \ FEBE = 0 \ BIP(B3) = 0 \ LOP = 0 \ NEWPTR = 0 \ PSE = 0 \ NSE = 0 \ WIS ALARMS \ SER = 0 \ FELCDP = 0 \ FEAlSP = 0 \ WLOS = 0 \ PLCD = 0 \ LFE VIP = 0 \ PBEC = 0 \ Active Alarms[All defects]: None \ Active Alarms[Highest Alarms]: None \ Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA PLOP WLOS Rx(K1/K2): 00/00 Tx(K1/K2): 00/00 S150 = 0, C2 = 0x1A \ PATH TRACE BUFFER: STABLE Remote J1 Byte : passing_string_from_localend BER thresholds: SD = 10e-6 SF = 10e-3 TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6</td>
</tr>
<tr>
<td></td>
<td>This command must be executed on the remotely connected SPA. The command output displays the string of J1 byte values transmitted from the other end of the WAN-PHY SPA to check the path.</td>
</tr>
<tr>
<td></td>
<td>In this example, the last line Remote J1 Byte, of the <strong>show controller wanphy 2/2/0</strong> command output indicates that the string value passing_string_from_localend has been sent from the other end of the WAN-PHY SPA.</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>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN-PHY controller. slot/subslot/port — The location of the interface.</td>
</tr>
<tr>
<td>controller wanphy slot/subslot/port</td>
<td></td>
</tr>
<tr>
<td>Example: Router(config)# controller wanphy 0/3/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures WAN-PHY controller processing.</td>
</tr>
<tr>
<td>wanphy {delay</td>
<td>flag</td>
</tr>
<tr>
<td>Example: Router(config-controller)# wanphy threshold b1-tca 6</td>
<td></td>
</tr>
</tbody>
</table>

- **delay**—Delays WAN-PHY alarm triggers.
- **flag**—Specifies byte values.
- **report-alarm**—Configures WAN-PHY alarm reporting.
- **threshold**—Sets BER threshold values.
  - **b1-tca**—Sets B1 alarm BER threshold.
  - **b2-tca**—Sets B2 alarm BER threshold.
  - **sd-ber**—Sets Signal Degrade BER threshold.
  - **sf-ber**—Sets Signal Fail BER threshold.
- **bit error rate**—Specifies bit error rate.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits controller configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# end</td>
<td></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.
!
! Specify the interface address.
!
Router(config)# interface gigabitethernet 0/0/1
!
! Configure an IP address.
!
Router(config-if)# ip address 192.168.50.1 255.255.255.0
!
! Start the interface.
!
Router(config-if)# no shut
```
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.

```
! Enter global configuration mode.
!
Router# configure terminal
!
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 0/0/1
!
! Configure the interface MTU.
!
```

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

Example: MTU Configuration

To save the configuration to NVRAM:

```
Router(config-if)# exit

Router# copy running-config startup-config
```
Example: VLAN Encapsulation

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

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

Note

VLANs are supported only on EVC service instances and Trunk EFP interfaces.
Using the Management Ethernet Interface

This chapter covers the following topics:

- Gigabit Ethernet Management Interface Overview, on page 133
- Gigabit Ethernet Port Numbering, on page 133
- IP Address Handling in ROMmon and the Management Ethernet Port, on page 134
- Gigabit Ethernet Management Interface VRF, on page 134
- Common Ethernet Management Tasks, on page 135

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 134.

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:
       Gi0
Address family ipv4 (Table ID = 4085 (0xFF5)):
   No Export VPN route-target communities
   No Import VPN route-target communities
   No import route-map
   No export route-map
   VRF label distribution protocol: not configured
   VRF label allocation mode: per-prefix
Address family ipv6 (Table ID = 503316481 (0x1E000001)):
   No Export VPN route-target communities
   No Import VPN route-target communities
   No import route-map
   No export route-map
   VRF label distribution protocol: not configured
   VRF label allocation mode: per-prefix
```
Setting a Default Route in the Management Ethernet Interface VRF

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

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

Setting the Management Ethernet IP Address

The IP address of the Management Ethernet port is set like the IP address on any other interface. Below are two simple examples of configuring an IPv4 address and an IPv6 address on the Management Ethernet interface.

**IPv4 Example**

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

**IPv6 Example**

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ipv6 address X:X:X:X::X
```

Telnetting over the Management Ethernet Interface

Telnetting can be done through the VRF using the Management Ethernet interface. In the following example, the router telnets to 172.17.1.1 through the Management Ethernet interface VRF:

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

Pinging over the Management Ethernet Interface

Pinging other interfaces using the Management Ethernet interface is done through the VRF. In the following example, the router pings the interface with the IP address of 172.17.1.1 through the Management Ethernet interface.

```
Router# ping vrf Mgmt-intf 172.17.1.1
```

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

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

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

**TFTP Example**

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

**FTP Example**

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

NTP Server

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

The following CLI provides an example of this procedure.

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

SYSLOG Server

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

The following CLI provides an example of this procedure.

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

SNMP-related services

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

The following CLI provides an example of this procedure:

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

Domain Name Assignment

The IP domain name assignment for the Management Ethernet interface is done through the VRF.
To define the default domain name as the Management Ethernet VRF interface, enter the `ip domain-name vrf Mgmt-intf domain` command.

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

**DNS service**

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

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

**RADIUS or TACACS+ Server**

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

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

```
Radius Server Group Configuration

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

Tacacs+ Server Group Example

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

**VTY lines with ACL**

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

```
Router(config)# line vty 0 4
Router(config-line)# access-class 90 in vrf-also
```
CHAPTER 9

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 139
- Verifying the Interface Configuration, on page 156
- Configuration Examples, on page 157

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>
<tbody>
<tr>
<td>Step 1 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>Step 2 card type {e1</td>
<td>t1} slot/subslot</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# card type e1 0/3</td>
<td>• t1—Specifies T1 connectivity of 1.536 Mbps. B8ZS is the default linecode for T1.</td>
</tr>
</tbody>
</table>
### PurposeCommand or Action

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
</table>

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

### Step 3

- **exit**

**Example:**

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

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

### Enabling T1 Controller

**Note**

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

To enable T1 controller:

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

### Configuring the Controller

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

**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>
</table>

**Step 1**

- `configure terminal`

**Example:**

```
Router# configure terminal
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>controller {t1</td>
<td>e1} slot/subslot/port</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller t1 0/3/0</td>
<td>• t1—Specifies the T1 controller.</td>
</tr>
<tr>
<td></td>
<td>• e1—Specifies the E1 controller.</td>
</tr>
<tr>
<td></td>
<td>• slot/subslot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The slot number is always 0.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>clock source {internal</td>
<td>line}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# clock source internal</td>
<td>• internal—Specifies that the internal clock source is used.</td>
</tr>
<tr>
<td></td>
<td>• line—Specifies that the network clock source is used. This is the default for T1 and E1.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>linecode {ami</td>
<td>b8zs</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# linecode ami</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 T1 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>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>For T1 Controllers:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# framing sf</td>
<td>• sf—Specifies Super Frame as the T1 frame type.</td>
</tr>
<tr>
<td></td>
<td>• esf—Specifies Extended Super Frame as the T1 frame type. This is the default for E1.</td>
</tr>
<tr>
<td></td>
<td>• crc4—Specifies CRC4 as the E1 frame type. This is the default for E1.</td>
</tr>
<tr>
<td></td>
<td>• no-crc4—Specifies no CRC4 as the E1 frame type.</td>
</tr>
<tr>
<td>For E1 Controllers:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# framing crc4</td>
<td>• internal—Specifies that the internal clock source is used.</td>
</tr>
<tr>
<td></td>
<td>• line—Specifies that the network clock source is used. This is the default for T1 and E1.</td>
</tr>
</tbody>
</table>
### Purpose

#### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>`cablelength {long</td>
<td>short}<code>Example:</code>cablelength long`</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>exit</code> Example: <code>exit</code></td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
</tbody>
</table>

### Verifying Controller Configuration

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

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

### Optional Configurations

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

### Configuring Framing

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

### SUMMARY STEPS

1. `configure terminal`
2. `controller {t1 | e1} slot/subslot/port`
3. For T1 controllers
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 {t1</td>
<td>e1} slot/subslot/port</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller t1 0/3/0</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The slot number is always 0.</td>
</tr>
<tr>
<td><strong>Step 3</strong> For T1 controllers</td>
<td>Sets the framing on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# framing sf</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>For E1 controllers</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# framing crc4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> 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>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying Framing Configuration

Use the show controllers command to verify the framing configuration:

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

Setting an IP Address

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

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

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></td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td>interface serial 0/subslot/port:channel-group</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface serial 0/0/1:0</td>
<td></td>
</tr>
</tbody>
</table>

Step 2 | Sets the IP address and subnet mask. |
| ip address address mask | |
| Example: | |
| Router(config-if)# ip address 192.0.2.1 255.255.255.0 | |

Step 3 | Exits configuration mode and returns to the EXEC command interpreter prompt. |
| exit | |
| Example: | |
| Router(config)# exit | |
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><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 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><strong>Step 3</strong> encapsulation {hdlc</td>
<td>ppp}</td>
</tr>
<tr>
<td>Example: Router(config-if)# encapsulation hdlc</td>
<td></td>
</tr>
</tbody>
</table>

- **hdlc**—High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
</tbody>
</table>

#### Verifying Encapsulation

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

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

### Configuring the CRC Size for T1 Interfaces

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

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

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

```bash
Router(config)# crc 32
```
**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> 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>Example:</td>
<td></td>
</tr>
</tbody>
</table>

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

| **Step 3** crc {16 | 32} | Selects the CRC size in bits. |
| Example: |         |
| Router(config-if)# crc 16 |         |

| **Step 4** exit | Exits configuration mode and returns to the EXEC command interpreter prompt. |
| 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
```
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>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></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><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>controller {t1</td>
<td>e1} slot/subslot/port</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller t1 0/3/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>channel-group {t1</td>
<td>e1} number {timeslots range</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# channel-group t1 1timeslots 1</td>
<td></td>
</tr>
<tr>
<td>unframed speed 56</td>
<td></td>
</tr>
</tbody>
</table>

- *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><code>copy running-config startup-config</code></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 150
- Running Bit Error Rate Testing, on page 152

### 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>
</tr>
</thead>
<tbody>
<tr>
<td>controller t1 slot/subslot/port</td>
<td>Selects the T1 controller and enter controller configuration mode</td>
</tr>
<tr>
<td></td>
<td>The slot number is always 0.</td>
</tr>
<tr>
<td>loopback diag</td>
<td>Sets a diagnostic loopback on the T1 line.</td>
</tr>
<tr>
<td>loopback local {line</td>
<td>payload}</td>
</tr>
<tr>
<td>loopback remote iboc</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>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 18: 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** | **Description**
--- | ---
loopback local | Loops the incoming receive signal back out to the transmitter. You can specify whether to use the line or payload.
local line | The incoming signal is looped back in the interface module using the framer’s line loopback mode. The framer does not reclock or reframe the incoming data. All incoming data is received by the interface module driver.
local payload | Loops the incoming signal back in the interface module using the payload loopback mode of the framer. The framer reclocks and reframes the incoming data before sending it back out to the network. When in payload loopback mode, an all 1s data pattern is received by the local HDLC receiver and the clock source is automatically set to line (overriding the clock source command). When the payload loopback is ended, the clock source returns to the last setting selected by the clock source command.
loopback remote iboc | Attempts to set the far-end T1 interface into line loopback. This command sends an in-band bit-oriented code to the far-end to cause it to go into line loopback. This command is available when using ESF or SF framing mode.
network line | Loops the incoming signal back in the interface module using the line loopback mode of the framer. The framer does not reclock or reframe the incoming data. All incoming data is received by the interface module driver.
network payload | Loops the incoming signal back using the payload loopback mode of the framer. The framer reclocks and reframes the incoming data before sending it back out to the network. When in payload loopback mode, an all 1s data pattern is received by the local HDLC receiver, and the clock source is automatically set to line (overriding the clock source command). When the payload loopback is ended, the clock source returns to the last setting selected by the clock source command.

---

**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:
Command: Task

controller \{e1 | t1\} slot/subslot/port

Selects the E1 or T1 controller and enters controller configuration mode.

Theslotnumberisalways0.

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 19: 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>show interface serial slot/subslot/port</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>clear counters serial slot/subslot/port</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 pesudowire went down. Now, AIS alarm are generated when the pesudowire goes down.

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

### Limitations of AIS

- AIS is not supported on CESoP and CEM over UDP.
- AIS is not supported on T1 mode. It is only supported on E1 mode.
- AIS is not supported on the 4-port OC3/STM-1 (OC-3) interface module (IM) and 32-port T1/E1 IM.
- AIS is supported only for MPLS core.
- AIS is not supported in pseudowire HSPW mode, when `graceful-restart` command is enabled.
• Removing the MPLS IP address from the core interfaces results in a delay of 10-12 minutes to notify the peer end. This depends on the negotiated forwarding hold timer between the routers, which is the least value of the configured LDP GR forwarding hold timer of the two routers.

• Supported CEM class range of de-jitter buffer size is between 1 to 32 ms.

• If the `shutdown unpowered` command is used to shut down the IM, an OIR must be performed to trigger the AIS alarms..

Core Failure Event Detection

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

• Shutdown of the PE controller or tug level.

• Removing the cross-connect feature.

• Removal of Gigabit Ethernet configuration, CEM configuration, controller configuration, or OSPF configuration.

• Shut off OSPF, CEM group, cross-connect, or Gigabit Ethernet interface.

• CE1 controller shut—AIS alarm is seen on the remote CE.

• PE1 controller shut—AIS alarm is seen on the remote CE.

• PE1 core shut—AIS alarm is seen on both the CEs.

• PE2 core shut—AIS alarm is seen on both the CEs.

• Pesudowire down—AIS alarm is seen on both the CEs.

• Core IGP down—AIS alarm is seen on both the CEs.

• Core LDP down—AIS alarm is seen on both the CEs.

Configuring AIS for Core Failure

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

Use the following procedure to enable AIS:

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

Verifying AIS Configuration

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

```
Router(config-controller)# show run | sec 0/3/0
controller E1 0/3/0
ais-core-failure
framing unframed
```
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
    180817311 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:

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

Example: CRC Configuration

The following example sets the CRC size for the interface:

```
! Specify the interface and enter interface configuration mode
! Router(config)# interface serial 2/0/0:0
!
! Specify the CRC size
! Router(config-if)# crc 32
!
! Exit interface configuration mode and return to global configuration mode
! Router(config-if)# exit
!
! Exit global configuration mode
```
Example: Facility Data Link Configuration

The following example configures Facility Data Link:

```plaintext
! 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:

```plaintext
! 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 10

Configuring Optical Interface Modules

This chapter describes the most common configurations for optical interface modules on the Cisco ASR 900 Series Router.

- Limitations and Restrictions, on page 159
- Configuring the Controller, on page 160
- Configuring SDH, on page 161
- Configuring SONET Mode, on page 169
- Configuring a CEM group, on page 173
- Configuring DS3 Clear Channel on OC-3 and OC-12 Interface Module, on page 176
- Optional Configurations, on page 181
- Managing Interface Naming, on page 184
- Configuring Multilink Point-to-Point Protocol, on page 185
- Configuring BERT, on page 189
- Configuring Automatic Protection Switching, on page 189
- TU-AIS Alarms, on page 189
- Verifying Interface Configuration, on page 191
- Troubleshooting, on page 191
- Configuration Examples, on page 196
- Additional Resources, on page 196

Limitations and Restrictions

- The 4-port OC3/STM-1 (OC-3) or 1-port OC12/STM-4 (OC-12) interface module is not supported on the ASR 900 RSP3 module.

- SDH framing mode is supported; SONET framing is supported beginning in Cisco IOS XE Release 3.8.

- On the OC-3 controller, framing mode is applicable on the interface module and per port. When framing mode is set to SONET, all the 4 ports on the interface module are enabled for SONET mode. Similarly, when framing mode is set to SDH mode, all 4 ports on the interface module are enabled for SDH mode.

- The OC-3 controller supports Asynchronous mode at the V5 byte level for Plesiochronous Digital Hierarchy (PDH). This value cannot be modified. If a mismatch occurs between the V5 byte, and the peer (remote router), loss of frames may be observed at the PDH level.

- HDLC, PPP, and MLPPP encapsulation are supported. In POS mode, HDLC and PPP are supported.
• ATM Layer 2 AAL0 and AAL5 encapsulation types are supported.
• E1 unframed encapsulation is not supported except using SAToP pseudowire interfaces.
• Unframed T1 is supported only for SATOP. E1 unframed is supported.
• MPLS-TP is not supported over Packet Over Sonet (POS) interfaces.
• Multicast is not supported on OC-12 interfaces.
• QoS is supported using MLPPP interfaces and egress POS interfaces.
• MPLS is supported only on PoS interfaces; MPLS on T1/E1 MLP is supported starting with Cisco IOS XE Release 3.9. MPLS over MLP is also supported.
• Channelization is not supported for serial interfaces. However, Channelization is supported for CEM at the DS0 level.
• DS3 Clear channel is supported only on CEM.
• BERT is not supported on DS0 and DS1 CEM. It is supported only on DS3 CEM mode.
• Configurations on the interface module must be completely removed before moving the interface module to a different slot on the router.
• Mixed configurations of features are not supported on the same port. For example, one OC-3 port can have only CEM (CESoP or SAToP) or ATM or IMA or DS3 configurations, but not a combination of these features on a single port.
• CEM is not supported across OC12/STM-4 interface module. CEM is supported on all four ports of OC-3/STM-1 interface module.
• If two CEM circuits are configured under the same OC-3 interface module, the circuits should not be configured with the same circuit-id. If two CEM circuits are configured on different OC-3 interface modules, then both circuits can be configured with the same circuit-id.
• By default, AIS-SHUT is enabled on the OC-3 SONET/SDH controller and port level shut down of SONET/SDH controller results in AIS alarm on peer node. To enable the LOS alarm on controller shut down, you must configure “no ais-shut” at SONET/SDH controller level.
• Maximum channels per OC-3/STM interface module for T1 interfaces is 336 for RSP1 and RSP2.
• Maximum channels per OC-3/STM interface module for E1 interfaces is 252 for RSP1 and RSP2.

Configuring the Controller

Starting with Cisco IOS XE Release 3.10, OC-3 and OC-12 is licensed. For information on licensing these interfaces, see Licensing the OC-3 and OC-12 Interface Modules.

Note

When the mode is changed, the interface module reloads.
Configuring SDH

The following sections describe how to configure SDH on the optical interface module:

Configuring SDH Mode

SDH T1 Mode

To configure SDH T1 mode, complete the following steps:

**SUMMARY STEPS**

1. framing sdh
2. aug mapping \{au-4\}
3. clock source \{internal | line\}
4. au-4 au-4# tug-3 tug-3#
5. In SDH framing in AU-4 mode:
6. SAToP CEM Group
7. exit
8. controller t1 interface-path-id
9. Creates a CEM group, IMA group, or channel-group on the T1 or E1 controller.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>framing sdh</td>
<td>Specifies SDH as the frame type.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# framing sdh</td>
<td></td>
</tr>
</tbody>
</table>
### SDH T1 Mode

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>aug mapping {au-4}</strong>&lt;br&gt;Example: <code>Router(config-controller)# aug mapping au-4</code>&lt;br&gt;<strong>Configures AUG mapping for SDH framing.</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**clock source {internal</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>au-4 au-4# tug-3 tug-3#</strong>&lt;br&gt;Example: <code>Router(config-controller)# au-4 1 tug-3 3</code>&lt;br&gt;<strong>Configures AU-4, and tributary unit groups, type 3 (TUG-3) for AU-4 and enters specific configuration mode.</strong>&lt;br&gt;- au-4#—Range is from 1 to 4 for OC-12 mode and 1 for OC-3 mode&lt;br&gt;- tug-3#—Range is from 1 to 3.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>In SDH framing in AU-4 mode:</strong>&lt;br&gt;Example: `Router(config-ctrlr-tug3)# mode {c-11</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>SAToP CEM Group</strong>&lt;br&gt;Example: <code>tug-2 1 e1 1 cem-group 1 unframed</code>&lt;br&gt;<strong>Creates a CEM group, IMA group, or channel-group for the AU-3 or AU-4. Valid values are:</strong>&lt;br&gt;- e1—1–3&lt;br&gt;- tug-3—1-3&lt;br&gt;- tug-2—1–7</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Router(config-ctrlr-tug3)# tug-2 1 e1 1 cem-group 1 unframed</td>
<td>• unframed—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.</td>
</tr>
<tr>
<td><strong>CESoPSN CEM Group</strong></td>
<td>Example:</td>
</tr>
<tr>
<td>tug-2 1 e1 1 cem-group 1 timeslots 1-31</td>
<td>Example:</td>
</tr>
<tr>
<td><strong>IMA Group</strong></td>
<td>Example:</td>
</tr>
<tr>
<td>tug-2 1 e1 1 ima-group 1</td>
<td>Example:</td>
</tr>
<tr>
<td><strong>Channel Group</strong></td>
<td>Example:</td>
</tr>
<tr>
<td>tug-2 1 e1 1 [[channel-group channel-group-number] [timeslots list-of-timeslots]]</td>
<td>Example:</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Exits controller configuration mode.</td>
</tr>
<tr>
<td>Router(config-controller)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 8**

```
controller t1 interface-path-id
```

**Example:**

```
Router(config-controller)# controller t1 0/1/1/0/0/0
```

**Step 9**

Creates a CEM group, IMA group, or channel-group on the T1 or E1 controller.

**Purpose**

**SAToP CEM Group**

```
Router(config-controller)# t1 cem-group 1 unframed
```

**CESoPSN CEM Group**

```
Router(config-controller)# t1 cem-group 1 timeslots 1-24
```

**Clear-Channel ATM**

```
Router(config-controller-tug3)# e1 1 atm
```

**IMA Group**

```
Router(config-controller-tug3)# e1 1 ima-group 1
```

**Channel Group**

```
Router(config-controller-tug3)# t1 2 channel-group 4

```

### What to do next

**Example**

The example configures SDH E1 mode:

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-4
Router(config-controller)# clock source internal
Router(config-controller)# au-4 1 tug-3 2
Router(config-controller-tug3)# tug-2 1 el 1 channel-group 1 timeslots 1-31
```
SDH T1 Mode

To configure SDH T1 mode, complete the following steps:

SUMMARY STEPS

1. framing sdh
2. aug mapping {au-3}
3. clock source {internal | line}
4. au-3 au-3#
5. In SDH framing in AU-4 mode:
6. SAToP CEM Group
7. exit
8. controller t1 interface-path-id
9. Creates a CEM group, IMA group, or channel-group on the T1 or E1 controller.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> framing sdh</td>
<td>Specifies SDH as the frame type.</td>
</tr>
<tr>
<td>Example: Router(config-controller)# framing sdh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> aug mapping {au-3}</td>
<td>Configures AUG mapping for SDH framing.</td>
</tr>
<tr>
<td>Example: Router(config-controller)# aug mapping au-3</td>
<td>Supports au-3 and au-4 aug mapping. The default setting is au-3.</td>
</tr>
<tr>
<td><strong>Step 3</strong> clock source {internal</td>
<td>line}</td>
</tr>
<tr>
<td>Example: Router(config-controller)# clock source line</td>
<td>• internal—Specifies that the internal clock source is used.</td>
</tr>
<tr>
<td></td>
<td>• line—Specifies that the network clock source is used. This is the default for T1 and E1.</td>
</tr>
<tr>
<td><strong>Step 4</strong> au-3 au-3#</td>
<td>Configures AU-3, and enters specific configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-controller)# au-3 au-3#</td>
<td>• au-3#—Range is from 1 to 12 for OC-12 mode. For OC-3 mode, the value is 1–3.</td>
</tr>
<tr>
<td><strong>Step 5</strong> In SDH framing in AU-4 mode:</td>
<td>(Optional) Configures mode of operation for AU-3 or AU-4 mode, where:</td>
</tr>
<tr>
<td>Example: mode {c-11</td>
<td>c-12</td>
</tr>
<tr>
<td>Example: Router(config-ctrlr-tug3)# mode {c-11</td>
<td>c-12</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>• c-11—Specifies an AU-3/AU-4 TUG-3 divided into seven TUG-2s. Each TUG-2 is then divided into four TU11s, each carrying a C-11 T1.</td>
</tr>
<tr>
<td>• c-12—Specifies an AU-3/AU-4 TUG-3 divided into seven TUG-2. Each TUG-2 is then divided into three TU12s, each carrying a C-12 E1.</td>
</tr>
<tr>
<td>• t3—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) T3.</td>
</tr>
<tr>
<td>• e3—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) E3.</td>
</tr>
<tr>
<td><strong>Note</strong> Only c-11 and c-12 are currently supported.</td>
</tr>
</tbody>
</table>

**Step 6**

**SAToP CEM Group**

| Example: tug-2 1 t1 1 cem-group 1 unframed                              |
| Example: tug-2 1 t1 1 cem-group 1 unframed                              |
| Example: tug-2 1 t1 1 cem-group 1 unframed                              |

**CESoPSN CEM Group**

| Example: tug-2 1 t1 1 cem-group 1 timeslots 1-31                        |
| Example: tug-2 1 t1 1 cem-group 1 timeslots 1-31                        |

**IMA Group**

| Example: tug-2 1 t1 1 ima-group 1                                        |
| Example: tug-2 1 t1 1 ima-group 1                                        |

Creates a CEM group, IMA group, or channel-group for the AU-3 or AU-4. Valid values are:

<p>| • t1—Range is from 1 to 12 for OC-12 mode. For OC-3 mode, the value is 1–3. |
| • tug-2—1–7                                                             |
| • unframed—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Channel Group</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>tug-2 1 e1 1 [(channel-group channel-group-number) [timeslots list-of-timeslots]]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ctrlr-tug3)# tug-2 1 t1</td>
<td>channel-group 0 timeslots 1-31</td>
</tr>
</tbody>
</table>

| Step 7 | | |
|---------| | |
| exit | | Exits controller configuration mode. |
| **Example:** | | |
| Router(config-controller)# exit | |         |

| Step 8 | | |
|---------| | |
| controller t1 interface-path-id | | Enters controller configuration mode for an individual T1 or E1. |
| **Example:** | | |
| Router(config-controller)# controller t1 0/1/1/0/0/0 | |         |

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Creates a CEM group, IMA group, or channel-group on the T1 or E1 controller.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAToP CEM Group</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-ctrlr)# t1 cem-group 1 unframed</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CESoPSN CEM Group</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-ctrlr)# t1 cem-group 1 timeslots 1-24</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Clear-Channel ATM</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-ctrlr-tug3)# e1 1 atm</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IMA Group</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-ctrlr-tug3)# e1 1 ima-group 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring SDH in POS Mode

Follow these steps to configure SDH in POS mode on the optical interface module.

#### SUMMARY STEPS

1. `controller sonet slot/subslot/port`
2. `framing {sonet | sdh}`
3. `aug mapping {au-3 | au-4}`
4. `au-4 au-4-number pos`
5. `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><code>controller sonet slot/subslot/port</code></td>
<td>Selects the controller to be configured.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# controller sonet 0/1/0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`framing {sonet</td>
<td>sdh}`</td>
</tr>
<tr>
<td>Example:</td>
<td>Note</td>
</tr>
<tr>
<td><code>Router(config)# controller sonet 0/1/0</code></td>
<td>The interface module reloads if the framing is changed.</td>
</tr>
</tbody>
</table>

---

**What to do next**

The example configures SDH T1 mode:

```console
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1

Router(config-ctrlr-au3)# tug-2 1 t1 1 channel-group 1 timeslots 1-31
```

For information about configuring optional features, see Optional Configurations, on page 181.
### Configuring SONET Mode

**Example**

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 pos
Router(config-controller)# end
```

For information about configuring optional features, see [Optional Packet over SONET Configurations](#), on page 182.

---

### Configuring SONET Mode

The following sections describe how to configure SONET mode on the optical interface module:

#### Configuring SONET Mode

To configure an interface module to use SONET mode:

**SUMMARY STEPS**

1. `controller sonet slot/subslot/port`
2. `framing {sonet | sdh}`
3. `clock source {line | internal}`
4. `sts-1 {1 - 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12}`
5. `vtg vtg-number t1 t1-line-number channel-group channel-group-no timeslots list-of-timeslots`
6. `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>Selects the controller to be configured.</td>
</tr>
<tr>
<td><code>controller sonet slot/subslot/port</code></td>
<td>Example: <code>Router(config)# controller sonet 0/1/0</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>Specifies SONET as the framing mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>`framing {sonet</td>
<td>sdh}`</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 3</strong></th>
<th>Specifies the clock source for the POS link, where:</th>
</tr>
</thead>
<tbody>
<tr>
<td>`clock source {line</td>
<td>internal}`</td>
</tr>
</tbody>
</table>
| • **line**—The link uses the recovered clock from the line. This is the default setting.  
  • **internal**—The link uses the internal clock source. |

<table>
<thead>
<tr>
<th><strong>Step 4</strong></th>
<th>Specifies the SONET Synchronous Transport Signal (STS) level and enters STS-1 configuration mode. The starting-number and ending-number arguments indicate the starting and ending STS value of the interface. For OC-3 interfaces, this value is 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>`sts-1 {1 - 12</td>
<td>1 - 3</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <strong>1-12</strong> value is supported only in OC-12 mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 5</strong></th>
<th>Configures the T1 on the VTG, where</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vtg vtg-number t1 t1-line-number channel-group channel-group-no timeslots list-of-timeslots</code></td>
<td>Example: <code>Router(config-if)# vtg 1 t1 1 channel-group 0 timeslots 1-24</code></td>
</tr>
</tbody>
</table>
| • **vtg-number**—Specifies the VTG number. The framing is 1-7  
  • **t1** **t1-line-number**—1-4  
  • **channel-group** **channel-group-no**—0-24  
  • **timeslots** **list-of-timeslots**—1-24 |

<table>
<thead>
<tr>
<th><strong>Step 6</strong></th>
<th>Exits configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Example: <code>Router(config-if)# end</code></td>
</tr>
</tbody>
</table>

### What to do next

The below example shows the configuration for the DS1 T1 serial interface:

```plaintext
Router# configure terminal  
Router(config)# controller sonet 0/1/0  
Router(config-controller)# framing sonet
```
Configuring SONET POS Mode

To configure an interface module to use SONET in POS mode, perform the following procedure.

### SUMMARY STEPS

1. `controller sonet slot/subslot/port`
2. `framing {sonet | sdh}`
3. `clock source {line | internal}`
4. `sts-1 {1-12 | 1-3 | 4-6 | 7-9 | 10-12} pos`
5. `exit`
6. Do one of the following:
   - `interface POS slot/subslot/port`
   - `interface POS slot/subslot/port.POS-interface`
   - `interface POS slot/subslot/port:POS-interface`
7. `encapsulation encapsulation-type {hdlc | ppp}`
8. `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><code>controller sonet slot/subslot/port</code></td>
<td>Selects the controller to be configured.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# <code>controller sonet 0/1/0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`framing {sonet</td>
<td>sdh}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# <code>framing sonet</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`clock source {line</td>
<td>internal}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# <code>clock source line</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• line—The link uses the recovered clock from the line. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• internal—The link uses the internal clock source.</td>
</tr>
</tbody>
</table>
### Configuring Optical Interface Modules

**Configuring SONET POS Mode**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies POS mode; starting-number and ending-number arguments indicate the starting and ending STS value of the POS interface. For OC-3 interfaces, this value is 1.</td>
</tr>
<tr>
<td>`sts-1 {1-12</td>
<td>1-3</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-controller)#</strong> <code>sts-1 1 - 3 pos</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits controller configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td><strong>Example:</strong> <strong>Router(config-controller)#</strong> <code>exit</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Use any of the following commands to access the POS interface.</td>
</tr>
<tr>
<td>Do one of the following:</td>
<td></td>
</tr>
<tr>
<td>• <code>interface POS slot/subslot/port</code></td>
<td></td>
</tr>
<tr>
<td>• <code>interface POS slot/subslot/port.POS-interface</code></td>
<td></td>
</tr>
</tbody>
</table>
| • `interface POS slot/subslot/port:POS-interface` | **Example:** **interface** `POS0/0/1`
| **Example:** | **interface** `POS0/0/1.1`
| **Example:** | **interface** `POS0/0/1:1`
| **Step 7** | Configures encapsulation; you can configure the following options: |
| `encapsulation encapsulation-type /hdlc | ppp/` | **Example:** **Router(config-if)#** `encapsulation hdlc` |
| **Step 8** | Exits configuration mode. |
| `end` | **Example:** **Router(config-if)#** `end` |

**What to do next**

**Example**

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sonet
Router(config-controller)# clock source line
Router(config-controller)# sts-1 1 - 3 pos
```
For information on optional SONET configurations, see Configuring SONET POS Mode, on page 171.

Configuring a CEM group

Configuring CEM Group in SONET Mode

To configure a T1 CEM group in SONET mode:

SUMMARY STEPS

1. enable
2. configure terminal
3. controller sonet slot/bay/port
4. framing {sonet | sdh}
5. sts-1 {1 - 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12}
6. mode {t3 | vt-15}
7. SATOP CEM
8. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted</td>
</tr>
<tr>
<td>2.</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3.</td>
<td>controller sonet slot/bay/port</td>
<td>Selects the controller to configure and enters controller configuration mode, where:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• slot/bay/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note The slot number is always 1 and the bay number is always 0.</td>
</tr>
<tr>
<td>4.</td>
<td>framing {sonet</td>
<td>sdh}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router(config)# controller sonet 0/4/1</td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router(config)# framing sonet</td>
</tr>
</tbody>
</table>

Router(config-controller)# exit
Router(config)# interface POS0/0/1
Router(config-if)# encapsulation hdlc
Router(config-if)# end
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> sts-1 {1 - 12</td>
<td>1 - 3</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-controller)# sts-1 1 - 3</td>
</tr>
<tr>
<td><strong>Step 6</strong> mode {t3</td>
<td>vt-15}</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ctrlr-sts1-3)# mode t3</td>
</tr>
<tr>
<td><strong>Step 7</strong> SATOP CEM</td>
<td>Configures the T1 on the VTG, where:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ctrlr-sts1-3)# cem-group 0 unframed</td>
</tr>
<tr>
<td>cem-group channel-number unframed</td>
<td>• vtg_number—Specifies the VTG number. For SONET framing, values are 1 to 7.</td>
</tr>
<tr>
<td>Example:</td>
<td>• tl_line_number—Specifies the T1 line number. Valid range is 1 to 4.</td>
</tr>
<tr>
<td>Router(config-ctrlr-sts1-3)# cem-group 0 unframed</td>
<td>• channel-number—Specifies the channel number. Valid range is 0 to 2015.</td>
</tr>
<tr>
<td>Example:</td>
<td>• list-of-timeslots—Specifies the list of timeslots. Valid range is from 1 to 24.</td>
</tr>
<tr>
<td>CeSOP CEM</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ctrlr-sts1-3)# vtg 1 tl 1 cem-group 1 timeslots 1-10</td>
</tr>
<tr>
<td>vtg vtg_number tl tl_line_number cem-group channel-number timeslots list-of-timeslots</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>What to do next</td>
<td></td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td></td>
</tr>
<tr>
<td>The example shows a CEM interface configuration:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller sonet 0/1/0</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# framing sonet</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# sts-1 1</td>
<td></td>
</tr>
</tbody>
</table>
Configuring CEM Group in SDH Mode

To configure CEM group in SDH mode:

SUMMARY STEPS

1. enable
2. configure terminal
3. controller sonet slot/bay/port
4. framing {sonet | sdh}
5. au-4 au-4# tug-3 tug-3#
6. mode {t3 | e3}
7. cem-group group-number {unframed}
8. end

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>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> controller sonet slot/bay/port</td>
<td>Selects the controller to configure and enters controller configuration mode, where:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller sonet 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> framing {sonet</td>
<td>sdh}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# framing sdh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> au-4 au-4# tug-3 tug-3#</td>
<td>Configures AU-4, and tributary unit groups, type 3 (TUG-3) for AU-4 and enters specific configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>In SDH framing mode, each TUG-3, and AU-4 can be configured with one of these commands.</td>
</tr>
<tr>
<td>Router(config-controller)# au-4 1 tug-3 1</td>
<td>Depending on currently configured AUG mapping setting, this command further specifies TUG-3, or AU-4 muxing. The CLI command parser enters into config-ctrlr-tug3 (SDH mode) or config-ctrlr-au3 (SDH mode), which makes only relevant commands visible.</td>
</tr>
</tbody>
</table>
### Configuring DS3 Clear Channel on OC-3 and OC-12 Interface Module

**Command or Action**

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>au-4#</strong>—Range is from 1 to 4. For OC-3 mode, the value is 1.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>• <strong>tug-3#</strong>—Range is from 1 to 3.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
</tr>
</tbody>
</table>

**Step 6**

**mode {t3 | e3}**

**Example:**

Router(config-ctrlr-tug3)# mode e3

Specifies the mode of operation.

• **t3**—Specifies an unchannelized (clear channel) T3.

• **e3**—Specifies a AU-3 or C3 that carries a unchannelized (DS3 clear channel) E3.

**Note** Only e3 mode is supported for SDH framing.

**Step 7**

**cem-group group-number {unframed}**

**Example:**

Router(config-ctrlr-tug3)# cem-group 4 unframed

Creates a CEM group.

• **unframed**—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.

**Step 8**

**end**

**Example:**

Router(config-ctrlr-tug3)# end

Exits controller configuration mode and returns to privileged EXEC mode.

---

**What to do next**

**Example**

Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# au-4 1 tug-3 1
Router(config-ctrlr-tug3)# mode e3
Router(config-ctrlr-tug3)# cem-group 4 unframed
Router(config-ctrlr-tug3)# end

---

**Configuring DS3 Clear Channel on OC-3 and OC-12 Interface Module**

**Note**

DS3 clear channel is supported only on CEM.
Configuring DS3 Clear Channel in SONET Mode

To configure DS3 clear channel in SONET mode:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `controller sonet slot/bay/port`
4. `framing {sonet | sdh}`
5. `clock source {line | internal}`
6. `sts-1 {1 - 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12}`
7. `mode {t3 | vt-15}`
8. `cem-group channel-number {unframed}`
9. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example: Enter your password if prompted |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Step 3** controller sonet slot/bay/port | Selects the controller to configure and enters controller configuration mode, where:  
  Example:  
  Note: The slot number is always 1 and the bay number is always 0. |
| **Step 4** framing {sonet | sdh} | Specifies SONET as the framing mode.  
  Example: |
| **Step 5** clock source {line | internal} | Specifies the clock source for the POS link, where:  
  Example:  
  * line—The link uses the recovered clock from the line. This is the default setting.  
  * internal—The link uses the internal clock source. |
| **Step 6** sts-1 {1 - 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12} | Specifies the SONET Synchronous Transport Signal (STS) level and enters STS-1 configuration mode. The |
### Configuring DS3 Clear Channel in SONET Mode

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Starting-number and ending-number arguments indicate the starting and ending STS value of the interface. For OC-3 interfaces, this value is 1. The 1-12 value is supported only in OC-12 mode.</td>
</tr>
<tr>
<td><code>Router(config-controller)# sts-1 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Specifies the mode of operation of an STS-1 path, where:</td>
</tr>
<tr>
<td>`mode {t3</td>
<td>vt-15}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>- <strong>vt-15</strong>—A STS-1 is divided into seven Virtual Tributary Groups (VTG). Each VTG is then divided into four VT1.5's, each carrying a T1.</td>
</tr>
<tr>
<td><code>Router(config-ctrlr-sts1)# mode t3</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Creates a CEM group.</td>
</tr>
<tr>
<td><code>cem-group channel-number {unframed}</code></td>
<td>- <strong>unframed</strong>—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-ctrlr-sts1)# cem-group 4 unframed</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Exits controller configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

#### What to do next

**Example**

The below example shows the configuration for a DS3 interface:

```bash
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sonet
Router(config-controller)# clock source line
Router(config-controller)# sts-1 1 - 3
Router(config-controller)# mode t3
Router(config-ctrlr-sts1)# cem-group 0 unframed
Router(config-controller)# end
```

**Configuration Example**

```bash
controller SONET 1/0/0
framing sonet
clock source internal

! sts-1 1
mode t3
cem-group 0 unframed

! sts-1 2
mode t3
cem-group 1 unframed
```
Configuring Optical Interface Modules

Configuring DS3 Clear Channel in SDH Mode

To configure DS3 clear channel in SDH mode:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `controller sonet slot/bay/port`
4. `framing {sonet | sdh}`
5. `clock source {line | internal}`
6. `aug mapping au-4`
7. `au-4 au-4# tug-3 tug-3#`
8. `mode e3`
9. `cem-group channel-number {unframed}`
10. `end`

### DETAIL STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Step 3** controller sonet slot/bay/port | Selects the controller to configure and enters controller configuration mode, where:  
  - slot/bay/port—Specifies the location of the interface. |
<p>| Example: Router(config)# controller sdh 0/1/0 | Note | The slot number is always 1 and the bay number is always 0. |
| <strong>Step 4</strong> framing {sonet | sdh} | Specifies SDH as the framing mode. |
| Example: Router(config-controller)# framing sdh | | |</p>
<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>clock source</strong> {line</td>
<td>internal}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>- line—The link uses the recovered clock from the line. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- internal—The link uses the internal clock source.</td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# <strong>clock source</strong> line</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

Router(config-controller)# clock source line

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>aug mapping au-4</strong></td>
<td>Configures AUG mapping for SDH framing.</td>
</tr>
<tr>
<td>Example:</td>
<td>If the AUG mapping is configured to be AU-4, then the following muxing, alignment, and mapping will be used:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TUG-3 &lt;--&gt; VC-4 &lt;--&gt; AU-4 &lt;--&gt; AUG.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# aug mapping au-4</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

Step 7  **au-4 au-4# tug-3 tug-3#**

**Example:**

Router(config-controller)# au-4 1 tug-3 1

**Configures AU-4, and tributary unit groups, type 3 (TUG-3) for AU-4 and enters specific configuration mode.**

In SDH framing mode TUG-3, and AU-4 can be configured with one of these commands.

Depending on currently configured AUG mapping setting, this command further specifies TUG-3, or AU-4 muxing. The CLI command parser enters into config-ctrlr-tug3 (SDH mode) or config-ctrlr-au3 (SDH mode), which makes only relevant commands visible.

- **au-4#**—Range is from 1 to 4. For OC-3 mode, the value is 1.
- **tug-3#**—Range is from 1 to 3.

**Note**

E1 can only be configured in the AU-4 mode.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mode e3</td>
<td>Specifies the mode of operation.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>- e3—Specifies a C3 that carries a unchannelized (DS3 clear channel) E3.</td>
</tr>
<tr>
<td></td>
<td>Router(config-ctrlr-au4)# mode e3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>cem-group</strong> channel-number {unframed}</td>
<td>Creates a CEM group.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>- unframed—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.</td>
</tr>
<tr>
<td></td>
<td>Router(config-ctrlr-au4)# cem-group 4 unframed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>end</strong></td>
<td>Exits controller configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**What to do next**

**Example**

Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# clock source line
Router(config-controller)# aug mapping au-4
Optional Configurations

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

Configuring the National Bit

When G.751 framing is used, bit 11 of the G.751 frame is reserved for national use and is set to 1 by default.

Note

Configure national bit 1 only when required for interoperability with your telephone company.

To set the national bit in the G.751 frame, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Router(config)# controller {t1 | e1} slot/subslot/port | Selects the controller to configure. 
  • t1—Specifies the T1 controller. 
  • e1—Specifies the E1 controller. 
  • slot/subslot/port—Specifies the location of the controller. |
| Router(config-controller)# national reserve {0 | 1} {0 | 1} {0 | 1} {0 | 1} {0 | 1} | Sets the national bit (the first bit): 
  • 0—Sets the international bit in the G.704 frame to 0. This is the default. 
  • 1—Sets the international bit in the G.704 frame to 1. |

Note

Sets the five national bits:
  • 0—Set to 0 when not crossing international borders. 
  • 1—Set to 1 when crossing international borders.

Verifying the National Bit

Use the show controllers command to verify the national bits:

```sh
router# show controllers E1
E1 6/0/0 is up.
```
Applique type is Channelized E1 - balanced
No alarms detected.
alarm-trigger is not set
Framing is CRC4, Line Code is HDB3, Clock Source is Line.
International Bit: 1, National Bits: 11111
Data in current interval (234 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
Total Data (last 5 15 minute intervals):
  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

Configuring the CRC Size for T1

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA uses a 16-bit cyclic redundancy check (CRC) by default, but also supports a 32-bit CRC. 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.

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

**SUMMARY STEPS**

1. `interface serial slot/subslot/port:channel-group`
2. `crc {16 | 32}`

**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><code>interface serial slot/subslot/port:channel-group</code></td>
<td>Selects the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# interface serial 0/0/1/1/1/1/0</code></td>
<td>• <code>slot/subslot/port:channel-group</code> — Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`crc {16</td>
<td>32}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# crc 16</code></td>
<td>• 16—16-bit CRC. This is the default.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Optional Packet over SONET Configurations

The following sections describe how to configure optional settings on a packet over SONET (POS) interface.
Encapsulation

**encapsulation encapsulation-type**

Configures encapsulation; you can configure the following options:

- HDLC
- PPP

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

**MTU Value**

**mtu bytes**

Configures the maximum packet size for an interface in bytes. The default packet size is 4470 bytes.

```
Router(config-if)# mtu 4000
```

**CRC Value**

**crc size-in-bits**

CRC size in bits. Valid values are 16 and 32. The default is 16.

```
Router(config-if)# crc 32
```

**Keepalive Value**

**keepalive [period [retries]]**

Specifies the frequency at which the Cisco IOS software sends messages to the other end of the line to ensure that a network interface is alive, where:

- **period**—Specifies the time interval in seconds for sending keepalive packets. The default is 10 seconds.
- **retries**—Specifies the number of times that the device continues to send keepalive packets without response before bringing the interface down. The default is 3 retries.

```
Router(config-if)# keepalive 9 4
```

**Bandwidth**

Use the following command to configure the bandwidth of a POS interface.

**bandwidth {kbps | inherit [kbps]}**

To set and communicate the current bandwidth value for an interface to higher-level protocols, use the **bandwidth** command in interface configuration mode. Valid values are from 1 to 10000000. You can apply the following keywords:

- **inherit**—Specifies how a subinterface inherits the bandwidth of its main interface.
- **receive**—Specifies the receive-side bandwidth.
Scrambling

Use the following command to enable scrambling on a POS interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pos scramble-atm</code></td>
<td>Enables scrambling on the interface.</td>
</tr>
</tbody>
</table>

C2 Flag

Use the following command to configure the C2 flag on a POS interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pos flag c2 value</code></td>
<td>Specifies the C2 byte field for the interface as defined in RFC 2615. Valid values are 0-255.</td>
</tr>
</tbody>
</table>

J1 Flag

Use the following command to configure the J1 flag on a POS interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pos flag j1 message word</code></td>
<td>Specifies the value of the J1 byte in the SONET Path OverHead (POH) column.</td>
</tr>
</tbody>
</table>

You can use the following commands to verify your configuration:

- `show interfaces pos`

Managing Interface Naming

The following sections describe how to manage interface naming on the Cisco ASR 900 Series Router optical interface module.

Identifying Slots and Subslot

To specify the physical address for controller or interface configuration, use the interface and controller sonet commands, where:

- **slot**—Specifies the chassis slot number where the interface module is installed; the slot number is always 0 for interface modules on the Cisco ASR 900 Series Router.
- **subslot**—Specifies the subslot where the interface module is installed.
- **port**—Specifies the SONET port number.

For example, if the optical interface module is installed in slot 0 of the chassis, the controller configuration address is specified as `controller sonet 0/0/0`.

For channelized configuration, the interface address format is: slot/subslot/port:channel-group, where:

- **channel-group**—Specifies the logical channel group assigned to the time slots within the T1 link.
Configuring Multilink Point-to-Point Protocol

Multilink Point-to-Point Protocol (MLPPP) allows you to combine interfaces which correspond to an entire T1 or E1 multilink bundle. You can choose the number of bundles and the number of T1 or E1 lines in each bundle in any combination of E1 and T1 member link interfaces.

This section describes how to configure MLPPP on the optical interface module and includes the following topics:

MLPPP Configuration Guidelines

When configuring MLPPP, consider the following guidelines:

• Only T1 and E1 links are supported in a bundle.
• Enable PPP encapsulation before configuring multilink-related commands.
• Interfaces can be grouped into the MLPPP bundle if they belong to same interface module.
• A group can have a maximum of 16 interfaces.
• Maximum MTU for MLPP is 9216. For serial links that are not part of MLPPP configuration, maximum MTU varies for OC-3 and T1/E1 interfaces. The MTU range is as follows:
  • OC-3: 64 to 7673
  • T1/E1: 64 to 9216

Creating a Multilink Bundle

To create a multilink bundle, use the following commands:

SUMMARY STEPS

1. configure terminal
2. interface multilink group-number
3. ip address address mask

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>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>interface multilink group-number</td>
<td>Creates a multilink interface and enters</td>
</tr>
<tr>
<td>Example:</td>
<td>multilink interface mode, where:</td>
</tr>
</tbody>
</table>
Assigning an Interface to a Multilink Bundle

To assign an interface to a multilink bundle, use the following commands:

**SUMMARY STEPS**

1. configure terminal
2. interface serial slot/subslot/port
3. encapsulation ppp
4. ppp multilink group group-number
5. end

**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> interface serial slot/subslot/port</td>
<td>Selects the interface to configure and enters interface configuration mode, where:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface serial</td>
<td>0/0/1.1/1/1:0</td>
</tr>
<tr>
<td><strong>Step 3</strong> encapsulation ppp</td>
<td>Enables PPP encapsulation.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# encapsulation</td>
<td>ppp</td>
</tr>
<tr>
<td><strong>Step 4</strong> ppp multilink group group-number</td>
<td>Assigns the interface to a multilink bundle, where:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp multilink</td>
<td>group 1</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td></td>
</tr>
</tbody>
</table>
What to do next

Repeat these commands for each interface you want to assign to the multilink bundle

Note

Router# configure terminal
Router(config)# controller SONET 0/0/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 1
Router(config-controller)# tug-2 1 e1 1 channel-group 0 timeslots 1-31
Router# configure terminal
Router(config)# interface multilink 1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ppp multilink endpoint string string1
Router(config)# interface serial 0/0/1.1/1/1/1:0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink group 1

Configuring Fragmentation Size and Delay on an MLPPP Bundle

To configure the fragmentation size on a multilink PPP bundle, use the following commands:

SUMMARY STEPS

1. configure terminal
2. interface multilink group-number
3. ppp multilink fragment size fragment-size
4. ppp multilink fragment-delay delay

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> interface multilink group-number</td>
<td>Creates a multilink interface and enters multilink interface mode, where:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface multilink 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ppp multilink fragment size fragment-size</td>
<td>Sets the fragmentation size in bytes. Fragmentation is disabled by default. Valid values are 42 to 65535 bytes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp multilink fragment size 512</td>
<td></td>
</tr>
</tbody>
</table>
Changing the Default Endpoint Discriminator

To override or change the default endpoint discriminator, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ppp multilink endpoint {hostname</td>
<td>ip IP-address</td>
</tr>
</tbody>
</table>

Disabling Fragmentation on an MLPPP Bundle

By default, PPP multilink fragmentation is enabled. To disable fragmentation on a multilink bundle, use the following commands:

SUMMARY STEPS

1. configure terminal
2. interface multilink group-number
3. ppp multilink fragment disable
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> interface multilink group-number</td>
<td>Specifies the multilink interface and enters multilink</td>
</tr>
<tr>
<td>Example:</td>
<td>interface mode, where:</td>
</tr>
<tr>
<td>Router(config)# interface multilink 1</td>
<td>• group-number—The group number for the multilink bundle.</td>
</tr>
<tr>
<td></td>
<td>Range 1-2147483647</td>
</tr>
<tr>
<td><strong>Step 3</strong> ppp multilink fragment disable</td>
<td>Disables PPP multilink fragmentation.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp multilink fragment disable</td>
<td></td>
</tr>
</tbody>
</table>

Configuring BERT

BERT (Bit-Error Rate Testing) is used for analyzing quality and for problem resolution of digital transmission equipment. BERT tests the quality of an interface by directly comparing a pseudorandom or repetitive test pattern with an identical locally generated test pattern.

The BERT operation is data-intensive. Regular data cannot flow on the path while the test is in progress. The path is reported to be in alarm state when BERT is in progress and restored to a normal state after BERT has been terminated.

The supported BERT patterns are $2^{15}$, $2^{23}$, all 0s and all 1s.

Configuring Automatic Protection Switching

For information on how to configure Automatic Protection Switching (APS) on the optical interface module, see the Time Division Multiplexing Configuration Guide.

TU-AIS Alarms

Tributary Unit-Alarm Indication Signal (TU-AIS) alarms are higher order alarms compared to the AIS alarms. Prior to Cisco IOS-XE Everest 16.6.1, the PDH AIS alarms were generated when the TDM circuits went down. But, the SDH devices are unable to detect the PDH AIS alarms. This feature enables the SDH device to detect the PDH AIS alarm. Effective Cisco IOS-XE Everest 16.6.1, TU-AIS alarms are generated and detected when the TDM circuits go down on the access layer of the network topology or a failure occurs in MPLS domain due to which SAToP connectivity goes down. TU-AIS alarms are supported on the OC3 IM in Cisco ASR 903 RSP1 and RSP2 modules according to TU-12 section as defined in ITU-G. 707 (8.3.2). TU-AIS means that all TU-12 (i.e. all 144B) carries all "1" according to ITU-T G.707 (6.2.4.1.3).
The following are some expected behaviour after configuring TU-AIS alarms:

• CE tug shut first displays AIS alarm and then TU-AIS alarms.
• After TU-AIS alarm gets cleared the RDI alarm is displayed for 11-12 seconds and gets cleared.
• If there is a change in dejitter on the CEM circuit and TU-AIS is not configured, it displays AIS alarms for 200-300 miliseconds. If TU-AIS is configured, it displays AIS alarms for 20-30 miliseconds.
• On cable pull in PE2 LOS is displayed and after connecting back it displays RDI and then clears.

Restrictions for TU-AIS Alarms

• TU-AIS is not supported on the CEMoUDP.
• The interface modules reset after you enable or disable the TU-AIS alarms under OC3 Controller.
• TU-AIS configuration takes effect on all 4 ports of A900-IMA40S IM.
• TU_AIS alarm verification can be done by only using ANT-20 analyzer. ASR903 cannot display this alarm.

Configuring TU-AIS Alarms

Use the following commands to configure TU-AIS alarms:

```plaintext
enable
configure terminal
controller sonet 0/1/2
tu-ais
end
```

Verification of TU-AIS Alarm Configuration

Use the `show run | se` command to verify the configuration of TU-AIS alarm:

```plaintext
PE#show run | se SONET 0/1/2
platform enable controller SONET 0/1/2
controller SONET 0/1/2
no ais-shut
TU-AIS
framing adh
clock source internal
aug mapping au-4
  au-4 1 tug-3 1
    mode c-12
  tug-2 1 e1 1 cem-group 555 unframed
  tug-2 1 e1 1 framing unframed
  !
au-4 1 tug-3 2
  mode c-12
  !
au-4 1 tug-3 3
  mode c-12
site1-PE#
```
Core Failure Event Detection

Effective Cisco IOS XE Everest 16.6.1, TU-AIS configuration can be used to detect core defects. This feature is applicable only on Cisco ASR 900 RSP2 Module. The core failure is detected in the following events:

- Shut on PE controller/tug level
- Unconfiguration of Xconnect
- Removal of GigE configuration, CEM configuration, controller configuration, or OSPF configuration
- Shut on OSPF, CEM group, Xconnect, or GigE interface

Verifying Interface Configuration

Besides using the `show running-configuration` command to display your Cisco ASR 900 Series Router configuration settings, you can use the `show interface serial` and the `show controllers sonet` commands to get detailed information on a per-port basis.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis on an optical interface module, use the `show interface serial` and `show controllers sonet` commands.

For examples of the show commands here, see the `Cisco IOS Interface and Hardware Component Command Reference`.

Troubleshooting

You can use the following commands to verify your configuration:

- `show cem circuit`—shows information about the circuit state, administrative state, the CEM ID of the circuit, and the interface on which it is configured. If `xconnect` is configured under the circuit, the command output also includes information about the attached circuit.
- `show cem circuit 0-504`—Displays the detailed information about that particular circuit.
- `show cem circuit summary`—Displays the number of circuits which are up or down per interface basis.
- `show controller sonet x/y/z`—Displays the alarm information.
- `show hw-module subslot transceiver`—Displays information about the optical transceiver
- `show mpls l2transport vc`—Displays the state of local and peer access circuits
- `show running configuration`—Shows detail on each CEM group
- `show xconnect all`—Displays the state of the pseudowire and local and peer access circuits
- `show interfaces pos`—Displays all the current interface processors and their interfaces.

The `show controllers` command output reports the following alarms:

- SLOS
- SLOF
- B1-TCA
- B2-TCA
When SLOS is reported, all the other alarms are masked.

Router(config-controller)# show controller sonet 0/5/2
SONET 0/5/2 is down.
   Hardware is A900-IMA4OS

Applique type is Channelized Sonet/SDH
Clock Source is Line, AUG mapping is AU4.

Multiplex Section:
   AIS = 6   RDI = 0   REI = 0   BIP(B2) = 0
Active Defects: None
Detected Alarms: SLOS SLOF LAIS B1-TCA B2-TCA......<shows all alarms reported>
Asserted/Active Alarms: SLOS B1-TCA B2-TCA..........<shows hierarchy>
Alarm reporting enabled for: SLOS SLOF SF B1-TCA B2-TCA
BER thresholds:  SF = 10e-3   SD = 10e-6
TCA thresholds:  B1 = 10e-6   B2 = 10e-6

To provide information about system processes, the Cisco IOS software includes an extensive list of EXEC commands that begin with the word show, which, when executed, display detailed tables of system information. Following is a list of some of the common show commands for the APS feature.

To display the information described, use these commands in privileged EXEC mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show aps</td>
<td>Displays information about the automatic protection switching feature.</td>
</tr>
<tr>
<td>Router# show controller sonet slot/port-adapter/port</td>
<td>Displays information about the hardware.</td>
</tr>
<tr>
<td>Router# show interfaces</td>
<td>Displays information about the interface.</td>
</tr>
</tbody>
</table>

For examples of the show commands here, see the Cisco IOS Interface and Hardware Component Command Reference.

Framing and Encapsulation Configuration Example

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

! Specify the controller and enter controller configuration mode
! Router(config)# controller sonet 6/0/0
! ! 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 6/0/0:0
!
! Specify the encapsulation protocol
!
Router(config-if)# encapsulation ppp
!
! Exit interface configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
Router#

National Bit Configuration Example

The following example sets the National Bits for the controller:

! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 6/0/0
!
! Set the national bits
!
Router(config-controller)#
national reserve 0 1 1 1 1 1
!
! Exit controller configuration mode and return to global configuration mode
!
Router(config-controller)# exit
!
! Exit global configuration mode
!
Router(config)# exit
Router#

CRC Configuration Example

The following example sets the CRC size for the interface:

! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 6/0/0:0
!
! Specify the CRC size
!
Router(config-if)# crc 32
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
Router#
Facility Data Link Configuration Example

The following example configures Facility Data Link:

```
! Specify the controller and enter controller configuration mode
! Router(config)# controller sonet 6/0/0
! ! 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
Router#
```

MLPPP Configuration Example

The following example creates a PPP Multilink bundle:

```
! Enter global configuration mode
! Router# configure terminal
! ! Create a multilink bundle and assign a group number to the bundle
! Router(config)# interface multilink 1
! ! Specify an IP address for the multilink group
! Router(config-if)# ip address 123.456.789.111 255.255.255.0
! ! Enable Multilink PPP
! Router(config-if)# ppp multilink
! ! Leave interface multilink configuration mode
! Router(config-if)# exit
! ! Specify the interface to assign to the multilink bundle
! Router(config)# interface serial 3/1/0:1
! ! Enable PPP encapsulation on the interface
! Router(config-if)# encapsulation PPP
! ! Assign the interface to a multilink bundle
! Router(config-if)# multilink-group 1
! ! Enable Multilink PPP
!```
MFR Configuration Example

The following example configures Multilink Frame Relay (MFR):

! Create a MFR interface and enter interface configuration mode
! Router(config)# interface mfr 49
! Assign the bundle identification (BID) name 'test' to a multilink bundle.
! Router(config-if)# frame-relay multilink bid test
! Exit interface configuration mode and return to global configuration mode
! Router(config-if)# exit
! Specify the serial interface to assign to a multilink bundle
! Router(config)# interface serial 5/1/3:0
! Creates a multilink Frame Relay bundle link and associates the link with a multilink bundle
! Router(config-if)# encapsulation frame-relay mfr 49
! Assigns a bundle link identification (LID) name with a multilink bundle link
! Router(config-if)# frame-relay multilink lid test
! Configures the interval at which the interface will send out hello messages
! Router(config-if)# frame-relay multilink hello 15
! Configures the number of seconds the interface will wait for a hello message acknowledgement before resending the hello message
! Router(config-if)# frame-relay multilink ack 6
! Configures the maximum number of times the interface will resend a hello message while waiting for an acknowledgement
! Router(config-if)# frame-relay multilink retry 5
! Exit interface configuration mode and return to global configuration mode
! Router(config-if)# exit
! Exit global configuration mode
Router(config)# exit

Configuration Examples

This section includes the following configuration examples:

Example of Cyclic Redundancy Check Configuration

The following example configures CRC on a T1 interface:

! Specify the interface to configure and enter interface configuration mode.
! Router(config)# interface serial 2/0/0.1
! ! Specify the CRC type.
! Router(config-if)# crc 32

Example of Facility Data Link Configuration

The following example configures FDL on a T1 interface:

! Specify the interface to configure and enter interface configuration mode.
! Router(config)# interface serial 1/0/0.2
! ! Specify the T1 number and select fdl.
! Router(config-controller)# t1 2 fdl ansi

Example of Invert Data on T1/E1 Interface

The following example inverts the data on the serial interface:

! Specify the interface to configure and enter interface configuration mode.
! Router(config)# interface serial 3/0/0.1/2/1:0
! ! Configure invert data.
! Router(config-if)# invert data

Additional Resources

For more information about configuring ATM, see

- Asynchronous Transfer Mode Configuration Guide, Cisco IOS XE Release 3S(ASR 900 Series)

For additional information on configuring optical interfaces, see

- Cisco IOS Asynchronous Transfer Mode Command Reference
• Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S
• Wide-Area Networking Configuration Guide Library, Cisco IOS XE Release 3S
CHAPTER 11

Configuring Serial Interfaces

This chapter configures the serial interface module (PN: A900-IMASER14A/S) Async R232 serial data using Transparent Pseudowire (PW) over MPLS network on the Cisco ASR 900 Series Router. 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 199
- Restrictions, on page 200
- How to Configure Serial Interface, on page 201
- Verifying the Serial Interface Configuration, on page 208
- Configuration Examples, on page 209

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.
Figure 9: Pseudowire Transport for Serial Interface

The A900-IMASER14A/S interface provides a direct connection between the Cisco ASR 903 router and external networks.

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

Note: Serial interfaces are not supported on the ASR 900 RSP3 Module.

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.
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 ASR900-IMA14A/S interface module.

### 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>
<tr>
<td><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>
</tbody>
</table>
| **Step 2** | **controller serial slot/subslot/port**  
Example: | Selects the controller to configure and enters controller configuration mode.  
• *slot/subslot/port*—Specifies the location of the interface. |
| | **controller**  
Router(config)# **controller serial 0/4/1**  
**Note**  
The slot number is always 0. |
| **Step 3** | **physical-layer async | sync**  
Example: | Configures the serial interface in async or sync mode.  
• *async*—Specifies async interface.  
• *sync*—Specifies sync interface. This is the default mode. |
| | **physical-layer async**  
Router(config-controller)# **physical-layer async** |
| **Step 4** | **exit**  
Example: | Exits configuration mode and returns to the EXEC command interpreter prompt. |
| | **exit**  
Router(config)# **exit** |

**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 Async Interface**

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. flowcontrol \{none | software | lock | in | out\} | hardware \{in | out\}  
7. parity \{even | mark | none | odd | space\}  
8. exit
## 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>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>Example:</code> <code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></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></td>
<td><code>Example:</code> <code>Router(config)# line 0/4/1</code></td>
<td><code>- slot/subslot/port</code>—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`databits {5</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td><code>Example:</code> <code>Router(config-line)# databits 8</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`stopbits {1</td>
<td>1.5</td>
</tr>
<tr>
<td></td>
<td><code>Example:</code> <code>Router(config-line)# stopbits 2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>speed speed-value</code></td>
<td>Specifies the serial interface speed. The valid range is from 300 to 230400. The default is 9600.</td>
</tr>
<tr>
<td></td>
<td><code>Example:</code> <code>Router(config-line)# speed 9600</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`flowcontrol /none</td>
<td>software [lock</td>
</tr>
<tr>
<td></td>
<td><code>Example:</code> <code>Router(config-line)# flowcontrol none</code></td>
<td><code>- none</code> <code>- software</code> <code>- hardware</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`parity {even</td>
<td>mark</td>
</tr>
<tr>
<td></td>
<td><code>Example:</code> <code>Router(config-line)# parity none</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>exit</code></td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td></td>
<td><code>Example:</code> <code>Router(config)# exit</code></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)# stophits 2
Router(config-line)# speed 9600
Router(config-line)# flow-control none
Router(config-line)# parity none
Router(config-line)# exit

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>
</table>
| **Step 1** configure terminal  
   **Example:** Router# configure terminal | Enters global configuration mode. |
| **Step 2** controller serial slot/bay/port  
   **Example:** Router(config)# controller serial 0/4/1 | Configures the controller.  
   *slot/subslot/port*—Specifies the location of the interface. |
| **Step 3** channel-group channel-group  
   **Example:** Router(config-controller)# channel-group 0 | Configures the channel group with specified NxDS0 time slots. |
| **Step 4** exit  
   **Example:** Router(config-controller)# exit | Exits configuration mode and returns to the EXEC command interpreter prompt. |

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.

*Note*  
L2TPv3 encapsulation is *not* supported on the Cisco ASR 900 Series router. Trans encapsulation is only supported in Cisco IOS XE Release 3.14S.

**SUMMARY STEPS**

1. **configure terminal**
2. **interface serial slot/bay/port**
3. **encapsulation {ppp | trans | sdmc}**
4. **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** | interface serial *slot/bay/port*  
*Example:*  
Router(config)# interface serial 0/4/1 |
| **Step 3** | encapsulation {ppp | trans | sdmc}  
*Example:*  
Router(config-if)# encapsulation trans |
| **Step 4** | exit  
*Example:*  
Router(config)# exit |
### Configuring Transparent Pseudowire (PW) Cross-Connect

**Example: Encapsulation**

```
Router# configure terminal
Router(config)# interface serial 0/4/1
Router(config-if)# encapsulation trans
Router(config-if)# exit
```

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

**Example: Transparent Pseudowire on Cross Connect**

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

Saving the Configuration

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

Use the following commands to verify the configuration the serial interface

- **show controllers serial slot/bay/port**

Use the **show controllers serial slot/bay/port** command to display serial interface configuration on the router.

```bash
Router# show controllers serial 0/1/0
Serial0/1/0 - (A900-IMASER14A/S) is up
Encapsulation : TRANSPARENT
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
dceTerminalTimingEnable: Off ignore_dtr: Off
serial_clockrate: 128000bps, serial_clock_index: 17
serial_restartdelay: 30000, serial_restartdelay_def: 30000
```

- **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.

```bash
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 128 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TRANSPARENT, loopback not set
Keepalive not supported
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:11:31
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
28058 packets input, 839125 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
209844 packets output, 1048985 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
```

- **show running-config interfaces 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 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 Se0/1/0(HDLC) UP mpls 1.1.1.1:1001 UP

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 trans
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 trans
xconnect 1.1.1.1 1001 encapsulation mpls
Enabling Support for Tunable DWDM-XFP-C

The dense wavelength-division multiplexing (DWDM) wavelengths of the DWDM-XFP-C module on the Cisco ASR 900 Series router is tunable. You can configure the DWDM ITU wavelengths using the `itu channel` command in the interface configuration mode. The `itu channel` command ensures that the traffic continues to flow.

Table 20: DWDM-XFP-C Wavelength Mapping, on page 211 contains the wavelength mapping information for the DWDM-XFP-C module.

Table 20: DWDM-XFP-C Wavelength Mapping

<table>
<thead>
<tr>
<th>Channel no</th>
<th>wavelength [nm]</th>
<th>Frequency [THz]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1561.79</td>
<td>191.95</td>
</tr>
<tr>
<td>2</td>
<td>1561.46</td>
<td>192</td>
</tr>
<tr>
<td>3</td>
<td>1560.98</td>
<td>192.05</td>
</tr>
<tr>
<td>4</td>
<td>1560.65</td>
<td>192.1</td>
</tr>
<tr>
<td>5</td>
<td>1560.17</td>
<td>192.15</td>
</tr>
<tr>
<td>6</td>
<td>1559.83</td>
<td>192.2</td>
</tr>
<tr>
<td>7</td>
<td>1559.35</td>
<td>192.25</td>
</tr>
<tr>
<td>8</td>
<td>1559.02</td>
<td>192.3</td>
</tr>
<tr>
<td>9</td>
<td>1558.54</td>
<td>192.35</td>
</tr>
<tr>
<td>10</td>
<td>1558.21</td>
<td>192.4</td>
</tr>
<tr>
<td>11</td>
<td>1557.73</td>
<td>192.45</td>
</tr>
<tr>
<td>12</td>
<td>1557.4</td>
<td>192.5</td>
</tr>
<tr>
<td>13</td>
<td>1556.92</td>
<td>192.55</td>
</tr>
<tr>
<td>14</td>
<td>1556.59</td>
<td>192.6</td>
</tr>
<tr>
<td>Channel no</td>
<td>wavelength [nm]</td>
<td>Frequency [THz]</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>15</td>
<td>1556.11</td>
<td>192.65</td>
</tr>
<tr>
<td>16</td>
<td>1555.79</td>
<td>192.7</td>
</tr>
<tr>
<td>17</td>
<td>1555.31</td>
<td>192.75</td>
</tr>
<tr>
<td>18</td>
<td>1554.98</td>
<td>192.8</td>
</tr>
<tr>
<td>19</td>
<td>1554.4</td>
<td>192.85</td>
</tr>
<tr>
<td>20</td>
<td>1554.17</td>
<td>192.9</td>
</tr>
<tr>
<td>21</td>
<td>1553.7</td>
<td>192.95</td>
</tr>
<tr>
<td>22</td>
<td>1553.37</td>
<td>193</td>
</tr>
<tr>
<td>23</td>
<td>1552.89</td>
<td>193.05</td>
</tr>
<tr>
<td>24</td>
<td>1552.57</td>
<td>193.1</td>
</tr>
<tr>
<td>25</td>
<td>1552.09</td>
<td>193.15</td>
</tr>
<tr>
<td>26</td>
<td>1551.76</td>
<td>193.2</td>
</tr>
<tr>
<td>27</td>
<td>1551.28</td>
<td>193.25</td>
</tr>
<tr>
<td>28</td>
<td>1550.96</td>
<td>193.3</td>
</tr>
<tr>
<td>29</td>
<td>1550.48</td>
<td>193.35</td>
</tr>
<tr>
<td>30</td>
<td>1550.16</td>
<td>193.4</td>
</tr>
<tr>
<td>31</td>
<td>1549.68</td>
<td>193.45</td>
</tr>
<tr>
<td>32</td>
<td>1549.35</td>
<td>193.5</td>
</tr>
<tr>
<td>33</td>
<td>1548.88</td>
<td>193.55</td>
</tr>
<tr>
<td>34</td>
<td>1548.55</td>
<td>193.6</td>
</tr>
<tr>
<td>35</td>
<td>1548.08</td>
<td>193.65</td>
</tr>
<tr>
<td>36</td>
<td>1548.75</td>
<td>193.7</td>
</tr>
<tr>
<td>37</td>
<td>1546.95</td>
<td>193.75</td>
</tr>
<tr>
<td>38</td>
<td>1546.95</td>
<td>193.8</td>
</tr>
<tr>
<td>39</td>
<td>1546.48</td>
<td>193.85</td>
</tr>
<tr>
<td>40</td>
<td>1546.16</td>
<td>193.9</td>
</tr>
<tr>
<td>41</td>
<td>1545.69</td>
<td>193.95</td>
</tr>
<tr>
<td>Channel no</td>
<td>wavelength [nm]</td>
<td>Frequency [THz]</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>42</td>
<td>1545.36</td>
<td>194</td>
</tr>
<tr>
<td>43</td>
<td>1544.89</td>
<td>194.05</td>
</tr>
<tr>
<td>44</td>
<td>1544.56</td>
<td>194.1</td>
</tr>
<tr>
<td>45</td>
<td>1544.09</td>
<td>194.15</td>
</tr>
<tr>
<td>46</td>
<td>1543.77</td>
<td>194.2</td>
</tr>
<tr>
<td>47</td>
<td>1543.3</td>
<td>194.25</td>
</tr>
<tr>
<td>48</td>
<td>1542.97</td>
<td>194.3</td>
</tr>
<tr>
<td>49</td>
<td>1542.5</td>
<td>194.35</td>
</tr>
<tr>
<td>50</td>
<td>1542.18</td>
<td>194.4</td>
</tr>
<tr>
<td>51</td>
<td>1541.71</td>
<td>194.45</td>
</tr>
<tr>
<td>52</td>
<td>1541.39</td>
<td>194.5</td>
</tr>
<tr>
<td>53</td>
<td>1540.92</td>
<td>194.55</td>
</tr>
<tr>
<td>54</td>
<td>1540.6</td>
<td>194.6</td>
</tr>
<tr>
<td>55</td>
<td>1540.13</td>
<td>194.65</td>
</tr>
<tr>
<td>56</td>
<td>1539.8</td>
<td>194.7</td>
</tr>
<tr>
<td>57</td>
<td>1539.34</td>
<td>194.75</td>
</tr>
<tr>
<td>58</td>
<td>1539.01</td>
<td>194.8</td>
</tr>
<tr>
<td>59</td>
<td>1538.55</td>
<td>194.85</td>
</tr>
<tr>
<td>60</td>
<td>1538.22</td>
<td>194.9</td>
</tr>
<tr>
<td>61</td>
<td>1537.76</td>
<td>194.95</td>
</tr>
<tr>
<td>62</td>
<td>1537.43</td>
<td>195</td>
</tr>
<tr>
<td>63</td>
<td>1536.97</td>
<td>195.05</td>
</tr>
<tr>
<td>64</td>
<td>1536.65</td>
<td>195.1</td>
</tr>
<tr>
<td>65</td>
<td>1536.18</td>
<td>195.15</td>
</tr>
<tr>
<td>66</td>
<td>1535.86</td>
<td>195.2</td>
</tr>
<tr>
<td>67</td>
<td>1535.396</td>
<td>195.25</td>
</tr>
<tr>
<td>68</td>
<td>1535.07</td>
<td>195.3</td>
</tr>
</tbody>
</table>
Configuring the DWDM-XFP-C Module

Perform the following procedure to configure the DWDM-XFP-C module.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface tengigabitethernet slot/port`
4. `itu channel number`

**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><code>enable</code></td>
<td>Enables the privileged EXEC mode. If prompted, enter your password.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# enable</code></td>
<td></td>
</tr>
</tbody>
</table>

- Configuring the DWDM-XFP-C Module, on page 214
**Purpose**

**Command or Action**

**Step 2**

configure terminal

*Example:*

Router# configure terminal

**Step 3**

interface tengigabitethernet slot/port

*Example:*

Router(config)# interface tengigabitethernet 0/3

**Step 4**

itu channel number

*Example:*

Router(config-if)# itu channel 28

---

### Verifying the ITU Configuration

The following example shows how to use the `show hw-module subslot` command to check an ITU configuration:

```
Router# show hw-module subslot 0/2 transceiver 0 idprom dump
Description = XFP optics (type 6)
Transceiver Type: = TUNABLE DWDM XFP (194)
Product Identifier (PID) = DWDM-XFP-C
Frequency Set for Tunable DWDM = 195.5 THz
Vendor Revision = 00
Serial Number (SN) = JFX1617800W
Vendor Name = CISCO-JDSU
Vendor OUI (IEEE company ID) = 00.01.9C (412)
CLEI code = IP9IAGGCAB
Cisco part number = 10-2544-02
Device State = Disabled.
XFP IDPROM Page 0x0:
  000: 0C 00 49 00 F8 00 46 00 FB 00
  010: 00 00 00 00 00 00 00 00 A6 04
  020: 09 C4 8C A0 13 88 9B 83 13 93
  030: 62 1F 1F 07 0F 8D 00 0A 09 CF
  040: 00 10 00 18 FF E8 00 0C FF F4
  050: 00 00 00 00 00 00 00 00 00 00
  060: 00 BF 25 1C 00 C4 00 00 01 F4
  070: 00 00 00 00 00 00 00 00 00 00
  080: 00 00 00 00 00 00 00 00 00 00
  090: 00 00 00 00 00 00 00 00 00 00
  100: 00 00 00 00 00 00 00 00 00 00
  110: E2 98 00 14 00 00 00 00 00 00
<<See byte 113, the hexa decimal equivalent for ITU channel 20>>
XFP IDPROM Page 0x1:
  120: 00 00 00 00 00 00 00 00 00 00
  122: 0C 98 07 00 00 00 00 00 00 00
XFP IDPROM Page 0x1:
  121: 0B 00 00 00 00 00 00 00 00 00
  122: 09 BF 00 00 00 00 00 00 00 00
  123: 00 00 00 00 00 00 00 00 00 00
  124: 00 00 00 00 00 00 00 00 00 00
  125: 00 00 00 00 00 00 00 00 00 00
  126: 00 00 00 00 00 00 00 00 00 00
  127: 00 00 00 00 00 00 00 00 00 00
  128: 0C 98 07 00 00 00 00 00 00 00
  129: 00 00 00 00 00 00 00 00 00 00
  130: 00 00 00 00 00 00 00 00 00 00
  131: 00 00 00 00 00 00 00 00 00 00
  132: 00 00 00 00 00 00 00 00 00 00
  133: 00 00 00 00 00 00 00 00 00 00
  134: 00 00 00 00 00 00 00 00 00 00
  135: 00 00 00 00 00 00 00 00 00 00
  136: 00 00 00 00 00 00 00 00 00 00
  137: 00 00 00 00 00 00 00 00 00 00
  138: 08 B4 63 71 50 00 00 00 00 9F
  139: 00 00 00 00 00 00 00 00 00 00
  140: 00 00 00 00 00 00 00 00 00 00
  141: 00 00 00 00 00 00 00 00 00 00
  142: 00 00 00 00 00 00 00 00 00 00
  143: 00 00 00 00 00 00 00 00 00 00
  144: 00 00 00 00 00 00 00 00 00 00
  145: 00 00 00 00 00 00 00 00 00 00
  146: 00 00 00 00 00 00 00 00 00 00
  147: 00 00 00 00 00 00 00 00 00 00
  148: 43 49 53 43 4F 2D 4A 44 53
```
Enabling Support for Tunable DWDM-XFP-C

Verifying the ITU Configuration
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 217
- Restrictions for Dying Gasp Support, on page 217
- Configuration Examples for Dying Gasp Support, on page 218
- Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations, on page 218
- Message Displayed on the Peer Router on Receiving Dying Gasp Notification, on page 220
- Displaying SNMP Configuration for Receiving Dying Gasp Notification, on page 220

Prerequisites for Dying Gasp Support

You must enable Ethernet OAM before configuring Simple Network Management Protocol (SNMP) for dying gasp feature. For more information, see Enabling Ethernet OAM on an Interface.

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 or removal of power supply cable.
- The dying gasp support feature cannot be configured using CLI. To configure hosts using SNMP, refer to the SNMP host configuration examples below.
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.
Dying Gasp Support for Loss of Power Supply via SNMP, Syslog and Ethernet OAM

Environmental Settings on the Network Management Server

```plaintext
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)# snmp-server host 7.0.0.166 vrf Mgmt-intf version 2c public udp-port 9800
Router(config)#
Router(config)# ^Z
Router#
```

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

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

```
Router#
System Bootstrap, Version 15.3(2r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012 by cisco Systems, Inc.
Compiled Wed 17-Oct-12 15:00
Current image running: Boot ROM
Last reset cause: PowerOn
UEA platform with 2097152 Kbytes of main memory
rommon 1 >
```

```
Dying Gasp Trap Received for the Power failure event:
-----------------------------------------------------
Trap on Host1
+++++++++++++++
snmp-server host = 7.0.0.149 (nms1-lnx) and SR_TRAP_TEST_PORT=6264
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
-----------------------------------------------------
```

```
Trap on Host2
+++++++++++++++
snmp-server host = 7.0.0.152 (nms2-lnx) and SR_TRAP_TEST_PORT=9988
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
-----------------------------------------------------
```

```
Trap on Host3
+++++++++++++++
snmp-server host = 7.0.0.166 (erbusnmp-dc-lnx) and SR_TRAP_TEST_PORT=9800
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
```
```
Message Displayed on the Peer Router on Receiving Dying Gasp Notification

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#
Configuring Pseudowire

This chapter provides information about configuring pseudowire (PW) features on the router.

- Pseudowire Overview, on page 221
- Limitations, on page 227
- Configuring CEM, on page 227
- Configuring CAS, on page 233
- Configuring ATM, on page 236
- Configuring Structure-Agnostic TDM over Packet (SAToP), on page 240
- Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN), on page 241
- Configuring a Clear-Channel ATM Pseudowire, on page 243
- Configuring an ATM over MPLS Pseudowire, on page 244
- Configuring an Ethernet over MPLS Pseudowire, on page 255
- Configuring Pseudowire Redundancy, on page 256
- Pseudowire Redundancy with Uni-directional Active-Active, on page 258
- Restrictions, on page 259
- Configuring Pseudowire Redundancy Active-Active—Protocol Based, on page 260
- Configuring the Working Controller for MR-APS with Pseudowire Redundancy Active-Active, on page 260
- Configuring the Protect Controller for MR-APS with Pseudowire Redundancy Active-Active, on page 261
- Verifying the Interface Configuration, on page 261
- Configuration Examples, on page 262

Pseudowire Overview

The following sections provide an overview of pseudowire support on the router.

Effective Cisco IOS XE Release 3.18S:

- BGP PIC with TDM Pseudowire is supported on the ASR 900 router with RSP2 module.
- BGP PIC for Pseudowires, with MPLS Traffic Engineering is supported on the ASR 900 router with RSP1 and RSP2 modules.

Starting Cisco IOS XE Release 3.18.1SP, Pseudowire Uni-directional Active-Active is supported on the RSP1 and RSP3 modules.
Limitations

If you are running Cisco IOS XE Release 3.17S, the following limitation applies:

- BGP PIC with TDM Pseudowire is supported only on the ASR 900 router with RSP1 module.

If you are running Cisco IOS XE Release 3.17S and later releases, the following limitations apply:

- Channel associated signaling (CAS) is not supported on the T1/E1 and OC-3 interface modules on the router.
- BGP PIC is not supported for MPLS/LDP over MLPPP and POS in the core.
- BGP PIC is not supported for Multi-segment Pseudowire or Pseudowire switching.
- BGP PIC is not supported for VPLS and H-VPLS.
- BGP PIC is not supported for IPv6.
- If BGP PIC is enabled, Multi-hop BFD should not be configured using the `bfd neighbor fall-over` command.
- If BGP PIC is enabled, `neighbor ip-address weight` command should not be configured.
- If BGP PIC is enabled, `bgp next-hop trigger delay 6` under the `address-family ipv4` command and `bgp next-hop trigger delay 7` under the `address-family vpnv4` command should be configured. For information on the configuration examples for BGP PIC–TDM, see Example: BGP PIC with TDM-PW Configuration, on page 264.
- If BGP PIC is enabled and the targeted LDP for VPWS cross-connect services are established over BGP, perform the following tasks:
  - configure Pseudowire-class (pw-class) with encapsulation "mpls"
  - configure `no status control-plane route-watch` under the pw-class
  - associate the pw-class with the VPWS cross-connect configurations

If you are running Cisco IOS-XE 3.18S, the following restrictions apply for BGP PIC with MPLS TE for TDM Pseudowire:

- MPLS TE over MLPPP and POS in the core is not supported.
- Co-existence of BGP PIC with MPLS Traffic Engineering Fast Reroute (MPLS TE FRR) is not supported.

Circuit Emulation Overview

Circuit Emulation (CEM) is a technology that provides a protocol-independent transport over IP networks. It enables proprietary or legacy applications to be carried transparently to the destination, similar to a leased line.

The Cisco ASR 903 Series Router supports two pseudowire types that utilize CEM transport: Structure-Agnostic TDM over Packet (SAToP) and Circuit Emulation Service over Packet-Switched Network (CESoPSN). The following sections provide an overview of these pseudowire types.
Starting with Cisco IOS XE Release 3.15, the 32xT1E1 and 8x T1/E1 interface modules support CEM CESoP and SATOP configurations with fractional timeslots.

With the 32xT1/E1 and 8xT1/E1 interface modules, the channelized CEM circuits configured under a single port (fractional timeslot) cannot be deleted or modified, unless the circuits created after the first CEM circuits are deleted or modified.

The following CEM circuits are supported on the 32xT1/E1 interface module:

**T1 mode**
- 192 CESOP circuits with fractional timeslot
- 32 CESOP circuit full timeslot
- 32 SATOP circuits.

**E1 mode**
- 256 CESOP circuit with fractional timeslot.
- 32 CESOP circuit full timeslot
- 32 SATOP circuit

---

**Structure-Agnostic TDM over Packet**

SAToP encapsulates time division multiplexing (TDM) bit-streams (T1, E1, T3, E3) as PWs over public switched networks. It disregards any structure that may be imposed on streams, in particular the structure imposed by the standard TDM framing.

The protocol used for emulation of these services does not depend on the method in which attachment circuits are delivered to the provider edge (PE) devices. For example, a T1 attachment circuit is treated the same way for all delivery methods, including copper, multiplex in a T3 circuit, a virtual tributary of a SONET/SDH circuit, or unstructured Circuit Emulation Service (CES).

In SAToP mode the interface is considered as a continuous framed bitstream. The packetization of the stream is done according to IETF RFC 4553. All signaling is carried out transparently as a part of a bit stream. **Figure 10: Unstructured SAToP Mode Frame Format, on page 223** shows the frame format in Unstructured SAToP mode.

**Figure 10: Unstructured SAToP Mode Frame Format**

<table>
<thead>
<tr>
<th>Encapsulation header</th>
<th>CE Control (4Bytes)</th>
<th>RTP (optional 12B)</th>
<th>CEoP Payload</th>
<th>Bytes 1-N</th>
</tr>
</thead>
</table>

#unique_347 unique_347_Connect_42_tab_1729930 shows the payload and jitter limits for the T1 lines in the SAToP frame format.
### Table 21: SAToP T1 Frame: Payload and Jitter Limits

<table>
<thead>
<tr>
<th>Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
<th>Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>960</td>
<td>320</td>
<td>10</td>
<td>192</td>
<td>64</td>
<td>2</td>
</tr>
</tbody>
</table>

#unique_347 unique_347_Connect_42_tab_1729963 shows the payload and jitter limits for the E1 lines in the SAToP frame format.

### Table 22: SAToP E1 Frame: Payload and Jitter Limits

<table>
<thead>
<tr>
<th>Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
<th>Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1280</td>
<td>320</td>
<td>10</td>
<td>256</td>
<td>64</td>
<td>2</td>
</tr>
</tbody>
</table>

For instructions on how to configure SAToP, see Configuring Structure-Agnostic TDM over Packet (SAToP), on page 240.

### Circuit Emulation Service over Packet-Switched Network

CESoPSN encapsulates structured TDM signals as PWs over public switched networks (PSNs). It complements similar work for structure-agnostic emulation of TDM bit streams, such as SAToP. Emulation of circuits saves PSN bandwidth and supports DS0-level grooming and distributed cross-connect applications. It also enhances resilience of CE devices due to the effects of loss of packets in the PSN.

CESoPSN identifies framing and sends only the payload, which can either be channelized T1s within DS3 or DS0s within T1. DS0s can be bundled to the same packet. The CESoPSN mode is based on IETF RFC 5086.

Each supported interface can be configured individually to any supported mode. The supported services comply with IETF and ITU drafts and standards.

Figure 11: Structured CESoPSN Mode Frame Format, on page 224 shows the frame format in CESoPSN mode.

#### Figure 11: Structured CESoPSN Mode Frame Format

![Frame Format](image)

Table 23: CESoPSN DS0 Lines: Payload and Jitter Limits, on page 225 shows the payload and jitter for the DS0 lines in the CESoPSN mode.
### Table 23: CESoPSN DS0 Lines: Payload and Jitter Limits

<table>
<thead>
<tr>
<th>DS0</th>
<th>Maximum Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
<th>Minimum Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>40</td>
<td>320</td>
<td>10</td>
<td>32</td>
<td>256</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>80</td>
<td>320</td>
<td>10</td>
<td>32</td>
<td>128</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>120</td>
<td>320</td>
<td>10</td>
<td>33</td>
<td>128</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>160</td>
<td>320</td>
<td>10</td>
<td>32</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>200</td>
<td>320</td>
<td>10</td>
<td>40</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>240</td>
<td>320</td>
<td>10</td>
<td>48</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>280</td>
<td>320</td>
<td>10</td>
<td>56</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>320</td>
<td>320</td>
<td>10</td>
<td>64</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>360</td>
<td>320</td>
<td>10</td>
<td>72</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>400</td>
<td>320</td>
<td>10</td>
<td>80</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>440</td>
<td>320</td>
<td>10</td>
<td>88</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>480</td>
<td>320</td>
<td>10</td>
<td>96</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>520</td>
<td>320</td>
<td>10</td>
<td>104</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>560</td>
<td>320</td>
<td>10</td>
<td>112</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>600</td>
<td>320</td>
<td>10</td>
<td>120</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>16</td>
<td>640</td>
<td>320</td>
<td>10</td>
<td>128</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>680</td>
<td>320</td>
<td>10</td>
<td>136</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>720</td>
<td>320</td>
<td>10</td>
<td>144</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>760</td>
<td>320</td>
<td>10</td>
<td>152</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>20</td>
<td>800</td>
<td>320</td>
<td>10</td>
<td>160</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>21</td>
<td>840</td>
<td>320</td>
<td>10</td>
<td>168</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>22</td>
<td>880</td>
<td>320</td>
<td>10</td>
<td>176</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>23</td>
<td>920</td>
<td>320</td>
<td>10</td>
<td>184</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>960</td>
<td>320</td>
<td>10</td>
<td>192</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>25</td>
<td>1000</td>
<td>320</td>
<td>10</td>
<td>200</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>26</td>
<td>1040</td>
<td>320</td>
<td>10</td>
<td>208</td>
<td>64</td>
<td>2</td>
</tr>
</tbody>
</table>
### Asynchronous Transfer Mode over MPLS

An ATM over MPLS (AToM) PW is used to carry Asynchronous Transfer Mode (ATM) cells over an MPLS network. It is an evolutionary technology that allows you to migrate packet networks from legacy networks, while providing transport for legacy applications. AToM is particularly useful for transporting 3G voice traffic over MPLS networks.

You can configure AToM in the following modes:

- **N-to-1 Cell**—Maps one or more ATM virtual channel connections (VCCs) or virtual permanent connection (VPCs) to a single pseudowire.
- **1-to-1 Cell**—Maps a single ATM VCC or VPC to a single pseudowire.
- **Port**—Maps a single physical port to a single pseudowire connection.

The Cisco ASR 903 Series Router also supports cell packing and PVC mapping for AToM pseudowires.

#### Note

This release does not support AToM N-to-1 Cell Mode or 1-to-1 Cell Mode.

For more information about how to configure AToM, see Configuring an ATM over MPLS Pseudowire, on page 244.

### Transportation of Service Using Ethernet over MPLS

Ethernet over MPLS (EoMPLS) PWs provide a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core network. EoMPLS PWs encapsulate Ethernet protocol data units (PDUs) inside MPLS packets and use label switching to forward them across an MPLS network. EoMPLS PWs are an evolutionary technology that allows you to migrate packet networks from legacy networks while providing transport for legacy applications. EoMPLS PWs also simplify provisioning, since the provider edge equipment only requires Layer 2 connectivity to the connected customer edge (CE) equipment. The Cisco ASR 903 Series Router implementation of EoMPLS PWs is compliant with the RFC 4447 and 4448 standards.

The Cisco ASR 903 Series Router supports VLAN rewriting on EoMPLS PWs. If the two networks use different VLAN IDs, the router rewrites PW packets using the appropriate VLAN number for the local network.

<table>
<thead>
<tr>
<th>DS0</th>
<th>Maximum Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
<th>Minimum Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>1080</td>
<td>320</td>
<td>10</td>
<td>216</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>28</td>
<td>1120</td>
<td>320</td>
<td>10</td>
<td>224</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>1160</td>
<td>320</td>
<td>10</td>
<td>232</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>30</td>
<td>1200</td>
<td>320</td>
<td>10</td>
<td>240</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>31</td>
<td>1240</td>
<td>320</td>
<td>10</td>
<td>248</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>32</td>
<td>1280</td>
<td>320</td>
<td>10</td>
<td>256</td>
<td>64</td>
<td>2</td>
</tr>
</tbody>
</table>

For instructions on how to configure SAToP, see Configuring Structure-Agnostic TDM over Packet (SAToP), on page 240.
For instructions on how to create an EoMPLS PW, see Configuring an Ethernet over MPLS Pseudowire, on page 255.

Limitations

If you are running Cisco IOS XE Release 3.17S, the following limitation applies:

• BGP PIC with TDM Pseudowire is supported only on the ASR 900 router with RSP1 module.

If you are running Cisco IOS XE Release 3.17S and later releases, the following limitations apply:

• Channel associated signaling (CAS) is not supported on the T1/E1 and OC-3 interface modules on the router.
• BGP PIC is not supported for MPLS/LDP over MLPPP and POS in the core.
• BGP PIC is not supported for Multi-segment Pseudowire or Pseudowire switching.
• BGP PIC is not supported for VPLS and H-VPLS
• BGP PIC is not supported for IPv6.
• If BGP PIC is enabled, Multi-hop BFD should not be configured using the bfd neighbor fall-over bfd command.
• If BGP PIC is enabled, neighbor ip-address weight weight command should not be configured.
• If BGP PIC is enabled, bgp nexthop trigger delay 6 under the address-family ipv4 command and bgp nexthop trigger delay 7 under the address-family vpnv4 command should be configured. For information on the configuration examples for BGP PIC–TDM, see Example: BGP PIC with TDM-PW Configuration, on page 264.
• If BGP PIC is enabled and the targeted LDP for VPWS cross-connect services are established over BGP, perform the following tasks:
  • configure Pseudowire-class (pw-class) with encapsulation "mpls"
  • configure no status control-plane route-watch under the pw-class
  • associate the pw-class with the VPWS cross-connect configurations

If you are running Cisco IOS-XE 3.18S, the following restrictions apply for BGP PIC with MPLS TE for TDM Pseudowire:

• MPLS TE over MLPPP and POS in the core is not supported.
• Co-existence of BGP PIC with MPLS Traffic Engineering Fast Reroute (MPLS TE FRR) is not supported.

Configuring CEM

This section provides information about how to configure CEM. CEM provides a bridge between a time-division multiplexing (TDM) network and a packet network, such as Multiprotocol Label Switching (MPLS). The
router encapsulates the TDM data in the MPLS packets and sends the data over a CEM pseudowire to the remote provider edge (PE) router. Thus, function as a physical communication link across the packet network.

The following sections describe how to configure CEM:

Note
Steps for configuring CEM features are also included in the Configuring Structure-Agnostic TDM over Packet (SAToP), on page 240 and Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN), on page 241 sections.

Configuration Guidelines and Restrictions
Not all combinations of payload size and dejitter buffer size are supported. If you apply an incompatible payload size or dejitter buffer size configuration, the router rejects it and reverts to the previous configuration.

Configuring a CEM Group
The following section describes how to configure a CEM group on the Cisco ASR 903 Series Router.

SUMMARY STEPS

1. enable
2. configure terminal
3. controller \{t1 | e1\} slot/subslot/port
4. cem-group group-number \{unframed | timeslots timeslot\}
5. end

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>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 3</strong> controller {t1</td>
<td>e1} slot/subslot/port</td>
</tr>
<tr>
<td>Example:</td>
<td>• Use the slot and port arguments to specify the slot number and port number to be configured.</td>
</tr>
<tr>
<td>Router(config)# controller t1 1/0</td>
<td>Note The slot number is always 0.</td>
</tr>
<tr>
<td><strong>Step 4</strong> cem-group group-number {unframed</td>
<td>timeslots timeslot}</td>
</tr>
</tbody>
</table>
### Purpose

**Example:**

```plaintext
Router(config-controller)# cem-group 6 timeslots 1-4,9,10
```

- **The group-number** keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30.
- Use the **unframed** keyword to specify that a single CEM channel is being created including all time slots and the framing structure of the line.
- Use the **timeslots** keyword and the **timeslot** argument to specify the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.

### Step 5

**end**

**Example:**

```plaintext
Router(config-controller)# end
```

Exits controller configuration mode and returns to privileged EXEC mode.

### Using CEM Classes

A CEM class allows you to create a single configuration template for multiple CEM pseudowires. Follow these steps to configure a CEM class:

**Note**

The CEM parameters at the local and remote ends of a CEM circuit must match; otherwise, the pseudowire between the local and remote PE routers will not come up.

**Note**

You cannot apply a CEM class to other pseudowire types such as ATM over MPLS.

### SUMMARY STEPS

1. enable
2. configure terminal
3. class cem cem-class
4. payload-size size | dejitter-buffer buffer-size | idle-pattern pattern
5. exit
6. interface cem slot/subslot
7. exit
8. exit

### 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>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&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**Step 2**
configure terminal
**Example:**
Router# configure terminal

Enters global configuration mode.

**Step 3**
class cem cem-class
**Example:**
Router(config)# class cem mycemclass

Creates a new CEM class

**Step 4**
payload-size size | dejitter-buffer buffer-size | idle-pattern pattern
**Example:**
Router(config-cem-class)# payload-size 512

Enter the configuration commands common to the CEM class. This example specifies a sample rate, payload size, dejitter buffer, and idle pattern.

**Step 5**
e
t**Example:**
Router(config-cem-class)# exit

Returns to the config prompt.

**Step 6**
interface cem slot/subslot
**Example:**
Router(config)# interface cem 0/0

Configure the CEM interface that you want to use for the new CEM class.

**Note**
The use of the `xconnect` command can vary depending on the type of pseudowire you are configuring.
**Configuring a Clear-Channel ATM Interface**

**Configuring CEM Parameters**

The following sections describe the parameters you can configure for CEM circuits.

*Note*

The CEM parameters at the local and remote ends of a CEM circuit must match; otherwise, the pseudowire between the local and remote PE routers will not come up.

**Configuring Payload Size (Optional)**

To specify the number of bytes encapsulated into a single IP packet, use the `pay-load-size` command. The `size` argument specifies the number of bytes in the payload of each packet. The range is from 32 to 1312 bytes.

Default payload sizes for an unstructured CEM channel are as follows:

- E1 = 256 bytes
- T1 = 192 bytes
- DS0 = 32 bytes
Default payload sizes for a structured CEM channel depend on the number of time slots that constitute the channel. Payload size (L in bytes), number of time slots (N), and packetization delay (D in milliseconds) have the following relationship: \( L = 8N\times D \). The default payload size is selected in such a way that the packetization delay is always 1 millisecond. For example, a structured CEM channel of 16xDS0 has a default payload size of 128 bytes.

The payload size must be an integer of the multiple of the number of time slots for structured CEM channels.

### Setting the Dejitter Buffer Size

To specify the size of the dejitter buffer used to compensate for the network filter, use the dejitter-buffer-size command. The configured dejitter buffer size is converted from milliseconds to packets and rounded up to the next integral number of packets. Use the size argument to specify the size of the buffer, in milliseconds. The range is from 1 to 32 ms; the default is 5 ms.

### Setting an Idle Pattern (Optional)

To specify an idle pattern, use the [no] idle-pattern pattern1 command. The payload of each lost CESoPSN data packet must be replaced with the equivalent amount of the replacement data. The range for pattern is from 0x0 to 0xFF; the default idle pattern is 0xFF.

### Enabling Dummy Mode

Dummy mode enables a bit pattern for filling in for lost or corrupted frames. To enable dummy mode, use the dummy-mode [last-frame | user-defined] command. The default is last-frame. The following is an example:

```
Router(config-cem)# dummy-mode last-frame
```

### Setting a Dummy Pattern

If dummy mode is set to user-defined, you can use the dummy-pattern pattern command to configure the dummy pattern. The range for pattern is from 0x0 to 0xFF. The default dummy pattern is 0xFF. The following is an example:

```
Router(config-cem)# dummy-pattern 0x55
```

**Note**

The dummy-pattern command is not supported on the following interface modules:

- 48-Port T3/E3 CEM interface module
- 48-Port T1/E1 CEM interface module
- 1-port OC-192 Interface module or 8-port Low Rate interface module

### Shutting Down a CEM Channel

To shut down a CEM channel, use the shutdown command in CEM configuration mode. The shutdown command is supported only under CEM mode and not under the CEM class.
Configuring CAS

This section provides information about how to configure Channel Associated Signaling (CAS).

Information About CAS

The CAS is a method of signaling, where the signaling information is carried over a signaling resource that is specific to a particular channel. For each channel there is a dedicated and associated signaling channel. The Cisco ASR Router with RSP2 module supports CAS with 8-port T1/E1 interface modules and is interoperable with 6-port Ear and Mouth (E&M) interface modules.

The Cisco ASR Router supports CAS only in the E1 mode for the 8-port T1/E1 interface cards. Use the `card type e1 slot/subslot` command to configure controller in the E1 mode.

In the E1 framing and signaling, each E1 frame supports 32 timeslots or channels. From the available timeslots, the timeslot 17 is used for signaling information and the remaining timeslots are used for voice and data. Hence, this kind of signaling is often referred as CAS.

In the E1 frame, the timeslots are numbered from 1 to 32, where the timeslot 1 is used for frame synchronization and is unavailable for traffic. When the first E1 frame passes through the controller, the first four bits of signaling channel (timeslot 17) are associated with the timeslot 2 and the second four bits are associated with the timeslot 18. In the second E1 frame, the first four bits carry signaling information for the timeslot 3 and the second four bits for the timeslot 19.

Configuring CAS

To configure CAS on the controller interface, perform the following steps:

**SUMMARY STEPS**

1. `configure terminal`
2. `controller e1 slot/subslot/port`
3. `cas`
4. `clock source internal`
5. `cem-group group-number timeslots time-slot-range`
6. `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>Enters the global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code> Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring CAS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> controller e1 slot/subslot/port</td>
<td>Enters controller configuration mode to configure the E1 interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# controller E1 0/4/2</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The CAS is supported only in the E1 mode. Use the <strong>card type e1 slot/subslot</strong> command to configure controller in the E1 mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> cas</td>
<td>Configures CAS on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# cas</td>
</tr>
<tr>
<td><strong>Step 4</strong> clock source internal</td>
<td>Sets the clocking for individual E1 links.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# clock source internal</td>
</tr>
<tr>
<td><strong>Step 5</strong> cem-group group-number timeslots time-slot-range</td>
<td>Creates a Circuit Emulation Services over Packet Switched Network circuit emulation (CESoPSN) CEM group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# cem-group 0 timeslots 1-31</td>
</tr>
<tr>
<td><strong>• cem-group</strong>—Creates a circuit emulation (CEM) channel from one or more time slots of a E1 line.</td>
<td></td>
</tr>
<tr>
<td><strong>• group-number</strong>—CEM identifier to be used for this group of time slots. For E1 ports, the range is from 0 to 30.</td>
<td></td>
</tr>
<tr>
<td><strong>• timeslots</strong>—Specifies that a list of time slots is to be used as specified by the time-slot-range argument.</td>
<td></td>
</tr>
<tr>
<td><strong>• time-slot-range</strong>—Specifies the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits the controller session and returns to the configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# end</td>
</tr>
</tbody>
</table>

### What to do next
You can configure CEM interface and parameters such as xconnect.
Verifying CAS Configuration

Use the `show cem circuit cem-group-id` command to display CEM statistics for the configured CEM circuits. If `xconnect` is configured under the circuit, the command output also includes information about the attached circuit.

Following is a sample output of the `show cem circuit` command to display the detailed information about CEM circuits configured on the router:

```
Router# show cem circuit 0
CEM0/3/0, ID: 0, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, T1/E1 state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 0 (In use: 0)
Payload Size: 32
Framing: Framed (DS0 channels: 1)
CEM Defects Set
None
Signalling: No CAS
RTP: No RTP
Ingress Pkts: 5001 Dropped: 0
Egress Pkts: 5001 Dropped: 0
CEM Counter Details
Input Errors: 0 Output Errors: 0
Pkts Missing: 0 Pkts Reordered: 0
Misorder Drops: 0 JitterBuf Underrun: 0
Error Sec: 0 Severly Errored Sec: 0
Unavailable Sec: 0 Failure Counts: 0
Pkts Malformed: 0 JitterBuf Overrun: 0
```

The `show cem circuit` command displays No CAS for the Signaling field. The No CAS is displayed since CAS is not enabled at the CEM interface level. The CAS is enabled for the entire port and you cannot enable or disable CAS at the CEM level. To view the CAS configuration, use the `show running-config` command.

Configuration Examples for CAS

The following example shows how to configure CAS on a CEM interface on the router:

```
Router# configure terminal
Router(config)# controller E1 0/4/2
Router(config-controller)# cas
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 0 timeslots 1
Router(config-controller)# exit
```
Configuring ATM

The following sections describe how to configure ATM features on the T1/E1 interface module:

### Configuring a Clear-Channel ATM Interface

To configure the T1 interface module for clear-channel ATM, follow these steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `controller {t1} slot/subslot/port`
4. `atm`
5. `end`

**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; enable</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# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>controller {t1} slot/subslot/port</code></td>
<td>Selects the T1 controller for the port you are configuring (where <code>slot/subslot</code> identifies the location and <code>/port</code> identifies the port).</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# controller t1 0/3/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>atm</code></td>
<td>Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is <code>atm/slot/subslot/port</code>.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-controller)# atm</td>
<td><strong>Note</strong> The slot number is always 0.</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-controller)# end</td>
<td></td>
</tr>
</tbody>
</table>
What to do next

To access the new ATM interface, use the `interface atm slot/subslot/port` command.

This configuration creates an ATM interface that you can use for a clear-channel pseudowire and other features. For more information about configuring pseudowires, see Configuring Pseudowire, on page 221

Configuring ATM IMA

Inverse multiplexing provides the capability to transmit and receive a single high-speed data stream over multiple slower-speed physical links. In Inverse Multiplexing over ATM (IMA), the originating stream of ATM cells is divided so that complete ATM cells are transmitted in round-robin order across the set of ATM links. Follow these steps to configure ATM IMA on the Cisco ASR 903 Series Router.

**Note**

ATM IMA is used as an element in configuring ATM over MPLS pseudowires. For more information about configuring pseudowires, see Configuring Pseudowire, on page 221

**Note**

The maximum ATM over MPLS pseudowires supported per T1/E1 interface module is 500.

To configure the ATM interface on the router, you must install the ATM feature license using the `license install atm` command. To activate or enable the configuration on the IMA interface after the ATM license is installed, use the `license feature atm` command.

For more information about installing licenses, see the Software Activation Configuration Guide, Cisco IOS XE Release 3S.

**Note**

You can create a maximum of 16 IMA groups on each T1/E1 interface module.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. card type \{t1 \| e1\} slot [bay]
4. controller \{t1 \| e1\} slot/subslot/port
5. clock source internal
6. ima group group-number
7. exit
8. interface ATM slot/subslot/IMA group-number
9. no ip address
10. atm bandwidth dynamic
11. no atm ilmi-keepalive
12. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| | Example: Router> enable | |
| **Step 2** | configure terminal | Enters global configuration mode. |
| | Example: Router# configure terminal | |
| **Step 3** | card type {t1 | e1} slot [bay] | Specifies the slot and port number of the E1 or T1 interface. |
| | Example: Router(config)# card type e1 0 0 | |
| **Step 4** | controller {t1 | e1} slot/subslot/port | Specifies the controller interface on which you want to enable IMA. |
| | Example: Router(config)# controller e1 0/0/4 | |
| **Step 5** | clock source internal | Sets the clock source to internal. |
| | Example: Router(config-controller)# clock source internal | |
| **Step 6** | ima group group-number | Assigns the interface to an IMA group, and set the scrambling-payload parameter to randomize the ATM cell payload frames. This command assigns the interface to IMA group 0.  
  **Note** This command automatically creates an ATM0/IMA0 interface.  
  To add another member link, repeat **Step 3** to **Step 6**. |
| | Example: Router(config-controller)# ima-group 0 scrambling-payload | |
| **Step 7** | exit | Exits the controller interface. |
| | Example: Router(config-controller)# exit | |
### Command or Action

**Step 8**

**interface ATM slot/subslot/IMA group-number**  
**Example:**

```
Router(config-if)# interface atm0/1/ima0
```

**Purpose:**  
Specify the slot location and port of IMA interface group.  
- **slot**—The location of the ATM IMA interface module.  
- **group-number**—The IMA group.  

The example specifies the slot number as 0 and the group number as 0.  

**Note**  
To explicitly configure the IMA group ID for the IMA interface, use the optional `ima group-id` command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. The system toggles the original IMA interface to select a different IMA group ID.

**Step 9**

**no ip address**  
**Example:**

```
Router(config-if)# no ip address
```

**Purpose:**  
Disables the IP address configuration for the physical layer interface.

**Step 10**

**atm bandwidth dynamic**  
**Example:**

```
Router(config-if)# atm bandwidth dynamic
```

**Purpose:**  
Specifies the ATM bandwidth as dynamic.

**Step 11**

**no atm ilmi-keepalive**  
**Example:**

```
Router(config-if)# no atm ilmi-keepalive
```

**Purpose:**  
Disables the Interim Local Management Interface (ILMI) keepalive parameters.  
ILMI is not supported on the router starting with Cisco IOS XE Release 3.15S.

**Step 12**

**exit**  
**Example:**

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

**Purpose:**  
Exits configuration mode.

---

**What to do next**

The above configuration has one IMA shorthaul with two member links (atm0/0 and atm0/1).
## BGP PIC with TDM Configuration

To configure the TDM pseudowires on the router, see Configuring CEM, on page 227.

To configure BGP PIC on the router, see IP Routing: BGP Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series).

See the configuration example, Example: BGP PIC with TDM Configuration, on page 262.

### Configuring Structure-Agnostic TDM over Packet (SAToP)

Follow these steps to configure SAToP on the Cisco ASR 903 Series Router:

#### SUMMARY STEPS

1. enable
2. configure terminal
3. controller \[t\|e\] slot/sublot
4. cem-group group-number \{unframed \| timeslots timeslot\}
5. interface cem slot/subslot
6. xconnect ip_address encapsulation mpls
7. exit

#### 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>• 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><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> controller [t|e] slot/sublot</td>
<td>Configures the T1 or E1 interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-controller)# controller t1 0/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> cem-group group-number {unframed | timeslots timeslot}</td>
<td>Assigns channels on the T1 or E1 circuit to the CEM channel. This example uses the unframed parameter to assign all the T1 timeslots to the CEM channel.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# cem-group 4 unframed</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface cem slot/subslot</td>
<td>Defines a CEM group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# interface CEM 0/4</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# no ip address</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# cem 4</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

**xconnect ip_address encapsulation mpls**

**Example:**

Router(config-if)# xconnect 10.10.2.204
encapsulation mpls

**Step 7**

**exit**

**Example:**

Router(config)# exit

---

**What to do next**

When creating IP routes for a pseudowire configuration, we recommend that you build a route from the cross-connect address (LDP router-id or loopback address) to the next hop IP address, such as `ip route 10.10.10.2 255.255.255.254 10.2.3.4`.

---

**Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. controller [e1 | t1] slot/subslot
4. cem-group group-number timeslots timeslots
5. exit
6. interface cem slot/subslot
7. xconnect ip_address encapsulation mpls
8. exit
9. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
  **Example:**  
  
  Router> enable |  
  - Enter your password if prompted. |
| **Step 2** | `configure terminal` | Enters global configuration mode.  
  **Example:**  
  
  Router# configure terminal |  
  - Enter your password if prompted. |
| **Step 3** | `controller [e1 | t1] slot/subslot` | Enters configuration mode for the E1 or T1 controller.  
  **Example:**  
  
  Router(config)# controller e1 0/0 |  
  - Enter your password if prompted. |
| **Step 4** | `cem-group group-number timeslots timeslots` | Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the `timeslots` parameter to assign specific timeslots to the CEM channel.  
  **Example:**  
  
  Router(config-controller)# cem-group 5 timeslots 1-24 |  
  - Enter your password if prompted. |
| **Step 5** | `exit` | Exits controller configuration.  
  **Example:**  
  
  Router(config-controller)# exit |  
  - Enter your password if prompted. |
| **Step 6** | `interface cem slot/subslot` | Defines a CEM channel.  
  **Example:**  
  
  Router(config)# interface CEM0/5 |  
  - Enter your password if prompted. |
| **Step 7** | `xconnect ip_address encapsulation mpls` | Binds an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 304 to the remote peer 10.10.2.204.  
  **Example:**  
  
  Router(config-if)# xconnect 10.10.2.204 encapsulation mpls |  
  - Enter your password if prompted. |
### Configuring a Clear-Channel ATM Pseudowire

To configure the T1 interface module for clear-channel ATM, follow these steps:

**SUMMARY STEPS**

1. `controller {t1} slot/subslot/port`
2. `atm`
3. `exit`
4. `interface atm slot/subslot/port`
5. `pvc vpi/vci`
6. `xconnect peer-router-id vcid {encapsulation mpls | pseudowire-class name`  
7. `end`

**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>controller {t1} slot/subslot/port</code></td>
<td>Selects the T1 controller for the port you are configuring. <strong>Note</strong> The slot number is always 0.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# controller t1 0/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>atm</code></td>
<td>Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is <code>atm/slot/subslot/port</code> . <strong>Note</strong> The slot number is always 0.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-controller)# atm</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>exit</code></td>
<td>Returns you to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-controller)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>interface atm slot/subslot/port</code></td>
<td>Selects the ATM interface in Step 2 .</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring an ATM over MPLS Pseudowire

ATM over MPLS pseudowires allow you to encapsulate and transport ATM traffic across an MPLS network. This service allows you to deliver ATM services over an existing MPLS network.

The following sections describe how to configure transportation of service using ATM over MPLS:

- Configuring the Controller, on page 244
- Configuring an IMA Interface, on page 245
- Configuring the ATM over MPLS Pseudowire Interface, on page 247

Configuring the Controller

**SUMMARY STEPS**

1. enable
2. configure terminal
3. card type {e1} slot/subslot
4. controller {e1} slot/subslot
5. clock source {internal | line}
6. ima-group group-number scrambling-payload
7. exit
## 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>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 3</strong> card type {e1} slot/subslot</td>
<td>Configures IMA on an E1 or T1 interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# card type e1 0 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> controller {e1} slot/subslot</td>
<td>Specifies the controller interface on which you want to enable IMA.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller e1 0/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> clock source {internal</td>
<td>line}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# clock source internal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ima-group group-number scrambling-payload</td>
<td>If you want to configure an ATM IMA backhaul, use the ima-group command to assign the interface to an IMA group. For a T1 connection, use the no-scrambling-payload to disable ATM-IMA cell payload scrambling; for an E1 connection, use the scrambling-payload parameter to enable ATM-IMA cell payload scrambling. The example assigns the interface to IMA group 0 and enables payload scrambling.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# ima-group 0 scrambling-payload</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring an IMA Interface

If you want to use ATM IMA backhaul, follow these steps to configure the IMA interface.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface ATM slot / IMA group-number
4. no ip address
5. atm bandwidth dynamic
6. no atm ilmi-keepalive
7. exit

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: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Router# configure terminal |

| **Step 3** interface ATM slot / IMA group-number | Specifies the slot location and port of IMA interface group. The syntax is as follows: |
| Example: Router(config-controller)# interface atm0/ima0 | • slot—The slot location of the interface module. |
| Example: Router(config-if)# | • group-number—The group number of the IMA group. |
| **Note** | The example specifies the slot number as 0 and the group number as 0. |

To explicitly configure the IMA group ID for the IMA interface, you may use the optional **ima group-id** command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. At the same, the system toggles the original IMA interface to select a different IMA group ID.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Disables the IP address configuration for the physical layer interface.</td>
</tr>
<tr>
<td><code>no ip address</code></td>
<td>Enables the IP address configuration for the physical layer interface.</td>
</tr>
<tr>
<td>Example: <code>Router(config-if)# no ip address</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies the ATM bandwidth as dynamic.</td>
</tr>
<tr>
<td><code>atm bandwidth dynamic</code></td>
<td>Enables the ATM bandwidth as dynamic.</td>
</tr>
<tr>
<td>Example: <code>Router(config-if)# atm bandwidth dynamic</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Disables the ILMI keepalive parameters.</td>
</tr>
<tr>
<td><code>no atm ilmi-keepalive</code></td>
<td>Enables the ILMI keepalive parameters.</td>
</tr>
<tr>
<td>Example: <code>Router(config-if)# no atm ilmi-keepalive</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Router(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

For more information about configuring IMA groups, see the Configuring ATM IMA, on page 237.

**Configuring the ATM over MPLS Pseudowire Interface**

You can configure ATM over MPLS is several modes according to the needs of your network. Use the appropriate section according to the needs of your network. You can configure the following ATM over MPLS pseudowire types:

- Configuring 1-to-1 VCC Cell Transport Pseudowire, on page 248—Maps a single VCC to a single pseudowire
- Configuring N-to-1 VCC Cell Transport Pseudowire, on page 249—Maps multiple VCCs to a single pseudowire
- Configuring 1-to-1 VPC Cell Transport, on page 249—Maps a single VPC to a single pseudowire
- Configuring ATM AAL5 SDU VCC Transport, on page 251—Maps a single ATM PVC to another ATM PVC
- Configuring a Port Mode Pseudowire, on page 252—Maps one physical port to a single pseudowire connection
- Optional Configurations, on page 253

**Note**

When creating IP routes for a pseudowire configuration, build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as `ip route 10.10.10.2 255.255.255.255 10.2.3.4`. 
Configuring 1-to-1 VCC Cell Transport Pseudowire

A 1-to-1 VCC cell transport pseudowire maps one ATM virtual channel connection (VCC) to a single pseudowire. Complete these steps to configure a 1-to-1 pseudowire.

Note
Multiple 1-to-1 VCC pseudowire mapping on an interface is supported.

Mapping a Single PVC to a Pseudowire

To map a single PVC to an ATM over MPLS pseudowire, use the `xconnect` command at the PVC level. This configuration type uses AAL0 and AAL5 encapsulations. Complete these steps to map a single PVC to an ATM over MPLS pseudowire.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface ATM slot / IMA group-number`
4. `pvc slot/subslot l2transport`
5. `encapsulation aal0`
6. `xconnect router_ip_address vcid encapsulation mpls`
7. `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>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

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

**Step 3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface ATM slot / IMA group-number</code></td>
<td>Configures the ATM IMA interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-controller)# interface atm0/ima0</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pvc slot/subslot l2transport</code></td>
<td>Defines a PVC. Use the <code>l2transport</code> keyword to configure the PVC as a layer 2 virtual circuit.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if-atm)# pvc 0/40 l2transport</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Pseudowire

Configuring N-to-1 VCC Cell Transport Pseudowire

An N-to-1 VCC cell transport pseudowire maps one or more ATM virtual channel connections (VCCs) to a single pseudowire. Complete these steps to configure an N-to-1 pseudowire.

### Configuring 1-to-1 VPC Cell Transport

A 1-to-1 VPC cell transport pseudowire maps one or more virtual path connections (VPCs) to a single pseudowire. While the configuration is similar to 1-to-1 VPC cell mode, this transport method uses the 1-to-1 VPC pseudowire protocol and format defined in RFCs 4717 and 4446. Complete these steps to configure a 1-to-1 VPC pseudowire.

Multiple 1-to-1 VCC pseudowire mapping on an interface is supported.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface ATM slot / IMA group-number
4. atm pvp vci l2transport
5. xconnect peer-router-id vcid {encapsulation mpls}
6. end

### DETAILED STEPS

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

**Step 2**

configure terminal

Example:

Router# configure terminal

Enters global configuration mode.

**Step 3**

interface ATM *slot* / IMA *group-number*

Example:

Router(config-controller)# interface atm0/ima0

Example:

Router(config-if)#

Example:

Configures the ATM IMA interface.

**Step 4**

atm pvp vpi l2transport

Example:

Router(config-if-atm)# atm pvp 10 l2transport

Example:

Router(config-if-atm-l2trans-pvp)#

Maps a PVP to a pseudowire.

**Step 5**

xconnect peer-router-id vcid {encapsulation mpls

Example:

Router(config-if-atm-l2trans-pvp)# xconnect 10.10.10.2 305 encapsulation mpls

Example:

Router(config-if-atm-l2trans-pvp-xconn)#

Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 305 to the remote peer 30.30.30.2.

**Step 6**

der

Example:

Router(config-if-atm-l2trans-pvp-xconn)# end

Example:

Exits the configuration mode.
Configuring ATM AAL5 SDU VCC Transport

An ATM AAL5 SDU VCC transport pseudowire maps a single ATM PVC to another ATM PVC. Follow these steps to configure an ATM AAL5 SDU VCC transport pseudowire.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface ATM slot / IMA group-number
4. atm pvp vpi l2transport
5. encapsulation aal5
6. xconnect peer-router-id vcid encapsulation mpls
7. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
|  | Example: Router> enable | |
| **Step 2** | configure terminal | Enters global configuration mode. |
|  | Example: Router# configure terminal | |
| **Step 3** | interface ATM slot / IMA group-number | Configures the ATM IMA interface. |
|  | Example: Router(config-controller)# interface atm0/ima0 | |
|  | Example: Router(config-if)# | |
| **Step 4** | atm pvp vpi l2transport | Configures a PVC and specifies a VCI or VPI. |
|  | Example: Router(config-if)# pvc 0/12 l2transport | |
|  | Example: Router(config-if-atm-l2trans-pvc)# | |
Configuring a Port Mode Pseudowire

Configuring Pseudowire

SUMMARY STEPS

1. enable
2. configure terminal
3. interface ATM slot / IMA group-number
4. xconnect peer-router-id vcid encapsulation mpls
5. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</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>configure terminal</td>
<td>Enters global configuration mode.</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 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface ATM slot / IMA group-number</td>
<td>Configures the ATM interface.</td>
<td>Configures the ATM interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# interface atm0/ima0</td>
<td></td>
</tr>
</tbody>
</table>
### Optional Configurations

You can apply the following optional configurations to a pseudowire link.

**Configuring Cell Packing**

Cell packing allows you to improve the efficiency of ATM-to-MPLS conversion by packing multiple ATM cells into a single MPLS packet. Follow these steps to configure cell packing.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface ATM slot / IMA group-number`
4. `atm mcpt-timers timer1 timer2 timer3`
5. `atm pvp vpi l2transport`
6. `encapsulation aal5`
7. `cell-packing maxcells mcpt-timer timer-number`
8. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| `enable`
| Example:
| `Router> enable` |
| Enables privileged EXEC mode.
| • Enter your password if prompted. |
### Optional Configurations

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example: Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the ATM interface.</td>
</tr>
<tr>
<td><code>interface ATM slot / IMA group-number</code></td>
<td>Example: Router(config-controller)# interface atm0/ima0</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Defines the three Maximum Cell Packing Timeout (MCPT) timers under an ATM interface. The three independent MCPT timers specify a wait time before forwarding a packet.</td>
</tr>
<tr>
<td><code>atm mcpt-timers timer1 timer2 timer3</code></td>
<td>Example: Router(config-if)# atm mcpt-timers 1000 2000 3000</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures a PVC and specifies a VCI or VPI.</td>
</tr>
<tr>
<td><code>atm pvp vpi l2transport</code></td>
<td>Example: Router(config-if)# pvc 0/12 l2transport</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Sets the PVC encapsulation type to AAL5.</td>
</tr>
<tr>
<td><code>encapsulation aal5</code></td>
<td>Example: Router(config-if-atm-l2trans-pvc)# encapsulation aal5</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Specifies the maximum number of cells in PW cell pack and the cell packing timer. This example specifies 20 cells per pack and the third MCPT timer.</td>
</tr>
<tr>
<td><code>cell-packing maxcells mcpt-timer timer-number</code></td>
<td>Example: Router(config-if-atm-l2trans-pvc)# cell-packing 20 mcpt-timer 3</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Example: Router(config-if-atm-l2trans-pvc)# end</td>
</tr>
</tbody>
</table>
Configuring an Ethernet over MPLS Pseudowire

Ethernet over MPLS PWs allow you to transport Ethernet traffic over an existing MPLS network. The router supports EoMPLS pseudowires on EVC interfaces.

For more information about Ethernet over MPLS Pseudowires, see Transportation of Service Using Ethernet over MPLS, on page 226.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. service instance number ethernet [name]
5. encapsulation {default | dot1q | priority-tagged | untagged}
6. xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class pw-class-name} [[pw-class pw-class-name] [sequencing {transmit | receive | both}]
7. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example:  
  Router> enable  
  • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Router# configure terminal |
| **Step 3** interface interface-id | Specifies the port on which to create the pseudowire and enters interface configuration mode. Valid interfaces are physical Ethernet ports.  
  Example:  
  Router(config)# interface gigabitethernet 0/0/4 |
| **Step 4** service instance number ethernet [name] | Configure an EFP (service instance) and enter service instance configuration) mode.  
  Example:  
  Router(config-if)# service instance 2 ethernet  
  • The number is the EFP identifier, an integer from 1 to 4000.  
  • (Optional) ethernet name is the name of a previously configured EVC. You do not need to use an EVC name in a service instance. |
### Configuring Pseudowire Redundancy

A backup peer provides a redundant pseudowire (PW) connection in the case that the primary PW loses connection; if the primary PW goes down, the Cisco ASR 903 Series Router diverts traffic to the backup PW. This feature provides the ability to recover from a failure of either the remote PE router or the link between the PE router and CE router.

**Figure 12: Pseudowire Redundancy, on page 257** shows an example of pseudowire redundancy.
You must configure the backup pseudowire to connect to a router that is different from the primary pseudowire.

Follow these steps to configure a backup peer:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. pseudowire-class [pw-class-name]
4. encapsulation mpls
5. interface serial slot/subslot/port
6. backup delay enable-delay {disable-delay | never}
7. xconnect router-id encapsulation mpls
8. backup peer peer-router-ip-address vcid [pw-class pw-class name]
9. 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>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</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><strong>Step 3</strong></td>
<td>Specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>pseudowire-class [pw-class-name]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# pseudowire-class mpls</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>encapsulation mpls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-pw-class)# encapsulation mpls</td>
</tr>
</tbody>
</table>

**Purpose**: Specifies MPLS encapsulation.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>interface serial slot/subslot/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# interface serial0/0</td>
</tr>
</tbody>
</table>

**Purpose**: Enters configuration mode for the serial interface.

**Note**: The slot number is always 0.

| Step 6 | backup delay enable-delay {disable-delay | never} |
|---|---|
| Example: | Router(config)# backup delay 0 10 |

**Purpose**: Configures the backup delay parameters.

Where:

- **enable-delay** — Time before the backup PW takes over for the primary PW.
- **disable-delay** — Time before the restored primary PW takes over for the backup PW.
- **never** — Disables switching from the backup PW to the primary PW.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>xconnect router-id encapsulation mpls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-if)# xconnect 10.10.10.2 101 encapsulation mpls</td>
</tr>
</tbody>
</table>

**Purpose**: Binds the Ethernet port interface to an attachment circuit to create a pseudowire.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>backup peer peer-router-ip-address vcid [pw-class pw-class name]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# backup peer 10.10.10.1 104 pw-class pw1</td>
</tr>
</tbody>
</table>

**Purpose**: Defines the address and VC of the backup peer.

<table>
<thead>
<tr>
<th>Step 9</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>

**Purpose**: Exits configuration mode.

---

## Pseudowire Redundancy with Uni-directional Active-Active

Pseudowire redundancy with uni-directional active-active feature configuration allows, pseudowires (PW) on both the working and protect circuits to remain in UP state to allow traffic to flow from the upstream. The **aps l2vpn-state detach** command and **redundancy all-active replicate** command is introduced to configure uni-directional active-active pseudowire redundancy.
In pseudowire redundancy Active-Standby mode, the designation of the active and standby pseudowires is decided either by the endpoint PE routers or by the remote PE routers when configured with MR-APS. The active and standby routers communicate via Protect Group Protocol (PGP) and synchronize their states. The PEs are connected to a Base Station Controller (BSC). APS state of the router is communicated to the Layer2 VPN, and is thereby coupled with the pseudowire status.

**Figure 13: Pseudowire Redundancy with MR-APS**

BSC monitors the status of the incoming signal from the working and protect routers. In the event of a switchover at the BSC, the BSC fails to inform the PE routers, hence causing traffic drops.

With pseudowire redundancy Active-Active configuration, the traffic from the upstream is replicated and transmitted over both the primary and backup pseudowires. PE routers forwards the received traffic to the working and protect circuits. The BSC receives the same traffic on both the circuits and selects the better Rx link, ensuring the traffic is not dropped.

**Figure 14: Pseudowire Redundancy with Uni-directional Active-Active**

If the ASR 900 router is configured with the `aps l2vpn-state detach` command but, the ASR 901 router is not enabled with `redundancy all-active replicate` command, the protect PW is active after APS switchover. On the ASR 901 router, the PW state is UP and the data path status displays standby towards protect node. On an APS switchover on the ASR 900 router, the status is not communicated to ASR 901 router, and the VC data path state towards the protect node remains in the standby state.

**Restrictions**

The following restrictions apply on the router:
• If the `aps l2vpn-state detach` command is enabled on the ASR 900 router, but the `redundancy all-active replicate` command *not* enabled on the ASR 901 router, the pseudowire status on the router displays UP, and the data path status for the protect node state displays Standby.

• After APS switchover on the ASR 900 router, the status is *not* communicated to ASR 901 router, and the virtual circuit data path state towards the protect node remains in the Standby state.

• The `aps l2vpn-state detach` command takes effect after a controller `shutdown` command, followed by a `no shutown` command is performed. Alternately, the command can be configured when the controller is in shut state.

• The `status peer topology dual-homed` command in pseudowire-class configuration mode should *not* be configured on the ASR 900 router, irrespective of unidirectional or bidirectional mode. The command *must* be configured on the ASR 901 router.

• Traffic outages from the BSC to the BTS on PGP and ICRM failures at the working Active node, is same as the configured hold time.

---

**Note**

APS switchover may be observed on the protect node, when PGP failure occurs on the working Active node.

• Convergence may be observed on performing a power cycle on the Active (whether on the protect or working) node. The observed convergence is same as the configured hold time.

### Configuring Pseudowire Redundancy Active-Active—Protocol Based

```
encapsulation mpls
status peer topology dual-homed

controller E1 0/1
  framing unframed
  cem-group 8 unframed
```

### Configuring the Working Controller for MR-APS with Pseudowire Redundancy Active-Active

The following configuration shows pseudowire redundancy active-active for MR-APS working controller:

```
controller sonet 0/1/0
  aps group 2
  aps adm
  aps working 1
  aps timers 1 3
  aps l2vpn-state detach
  aps hspw-icrm-grp 1
```
Configuring the Protect Controller for MR-APS with Pseudowire Redundancy Active-Active

Following example shows pseudowire redundancy active-active on MR-APS protect controller:

```
controller sonet 0/1/0
aps group 2
aps adm
aps unidirectional
aps protect 10 10.10.10.1
aps timers 1 3
aps l2vpn-state detach
aps hspw-icrm-grp 1
```

Verifying the Interface Configuration

You can use the following commands to verify your pseudowire configuration:

- **show cem circuit** — Displays information about the circuit state, administrative state, the CEM ID of the circuit, and the interface on which it is configured. If `xconnect` is configured under the circuit, the command output also includes information about the attached circuit.

```
Router# show cem circuit

<0-504> CEM ID
detail Detailed information of cem ckt(s)
interface CEM Interface
summary Display summary of CEM ckts
| Output modifiers

Router# show cem circuit

<table>
<thead>
<tr>
<th>CEM Int.</th>
<th>ID</th>
<th>Line</th>
<th>Admin</th>
<th>Circuit</th>
<th>AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEM0/1/0</td>
<td>1</td>
<td>UP</td>
<td>UP</td>
<td>ACTIVE</td>
<td>--/--</td>
</tr>
<tr>
<td>CEM0/1/0</td>
<td>2</td>
<td>UP</td>
<td>UP</td>
<td>ACTIVE</td>
<td>--/--</td>
</tr>
<tr>
<td>CEM0/1/0</td>
<td>3</td>
<td>UP</td>
<td>UP</td>
<td>ACTIVE</td>
<td>--/--</td>
</tr>
<tr>
<td>CEM0/1/0</td>
<td>4</td>
<td>UP</td>
<td>UP</td>
<td>ACTIVE</td>
<td>--/--</td>
</tr>
<tr>
<td>CEM0/1/0</td>
<td>5</td>
<td>UP</td>
<td>UP</td>
<td>ACTIVE</td>
<td>--/--</td>
</tr>
</tbody>
</table>
```

- **show cem circuit** — Displays the detailed information about that particular circuit.

```
Router# show cem circuit 1

CEM0/1/0, ID: 1, Line State: UP, Admin State: UP, Ckt State: ACTIVE
Idle Pattern: 0xFF, Idle cas: 0x8, Dummy Pattern: 0xFF
Dejitter: 5, Payload Size: 40
Framing: Framed, (DS0 channels: 1-5)
Channel speed: 56
CEM Defects Set
Excessive Pkt Loss Rate Packet Loss
Signalling: No CAS
Ingress Pkts: 25929 Dropped: 0
Egress Pkts: 0 Dropped: 0
CEM Counter Details
```
Configuration Examples

The following sections contain sample pseudowire configurations.

Example: CEM Configuration

The following example shows how to add a T1 interface to a CEM group as a part of a SAToP pseudowire configuration. For more information about how to configure pseudowires, see Configuring Pseudowire, on page 221

This section displays a partial configuration intended to demonstrate a specific feature.

```
controller T1 0/0/0
   framing unframed
   clock source internal
   linecode b8zs
   cablelength short 110
   cem-group 0 unframed
   interface CEM0/0/0
   no ip address
   cem 0
   xconnect 18.1.1.1 1000 encapsulation mpls
```

Example: BGP PIC with TDM Configuration

CEM Configuration

```
pseudowire-class pseudowire1
   encapsulation mpls
   control-word
   no status control-plane route-watch
!
controller SONET 0/2/3
```
description connected to CE2 SONET 4/0/0
framing sdh
clock source line
aug mapping au-4
!
au-4 1 tug-3 1
  mode c-12
  tug-2 1 e1 1 cem-group 1101 unframed
tug-2 1 e1 1 framing unframed
tug-2 1 e1 2 cem-group 1201 timeslots 1-10
!
au-4 1 tug-3 2
  mode c-12
  tug-2 5 e1 1 cem-group 1119 unframed
tug-2 5 e1 1 framing unframed
tug-2 5 e1 2 cem-group 1244 timeslots 11-20
!
au-4 1 tug-3 3
  mode c-12
  tug-2 5 e1 3 cem-group 1130 unframed
tug-2 5 e1 3 framing unframed
tug-2 7 e1 3 cem-group 1290 timeslots 21-30
!
interface CEM0/2/3
no ip address
cem 1101
  xconnect 17.1.1.1 1101 encapsulation mpls pw-class pseudowire1
  cem 1201
  xconnect 17.1.1.1 1201 encapsulation mpls pw-class pseudowire1
  cem 1119
  xconnect 17.1.1.1 1119 encapsulation mpls pw-class pseudowire1
  cem 1244
  xconnect 17.1.1.1 1244 encapsulation mpls pw-class pseudowire1
  cem 1130
  xconnect 17.1.1.1 1130 encapsulation mpls pw-class pseudowire1
  cem 1290
  xconnect 17.1.1.1 1290 encapsulation mpls pw-class pseudowire1

**BGP PIC Configuration**

cef table output-chain build favor convergence-speed
!
router bgp 1
bgp log-neighbor-changes
bgp graceful-restart
neighbor 18.2.2.2 remote-as 1
neighbor 18.2.2.2 update-source Loopback0
neighbor 18.3.3.3 remote-as 1
neighbor 18.3.3.3 update-source Loopback0
!
address-family ipv4
  bgp additional-paths receive
  bgp additional-paths install
  bgp nexthop trigger delay 0
  network 17.5.5.5 mask 255.255.255.255
  neighbor 18.2.2.2 activate
  neighbor 18.2.2.2 send-community both
  neighbor 18.2.2.2 send-label
neighbor 18.3.3.3 activate
neighbor 18.3.3.3 send-community both
neighbor 18.3.3.3 send-label
exit-address-family

Example: BGP PIC with TDM-PW Configuration

This section lists the configuration examples for BGP PIC with TDM and TDM–Pseudowire.

The below configuration example is for BGP PIC with TDM:

```
router bgp 1
neighbor 18.2.2.2 remote-as 1
neighbor 18.2.2.2 update-source Loopback0
neighbor 18.3.3.3 remote-as 1
neighbor 18.3.3.3 update-source Loopback0

address-family ipv4
  bgp additional-paths receive
  bgp additional-paths install
  bgp nexthop trigger delay 6
neighbor 18.2.2.2 activate
neighbor 18.2.2.2 send-community both
neighbor 18.2.2.2 send-label
neighbor 18.3.3.3 activate
neighbor 18.3.3.3 send-community both
neighbor 18.3.3.3 send-label
neighbor 26.1.1.2 activate
exit-address-family

address-family vpnv4
  bgp nexthop trigger delay 7
neighbor 18.2.2.2 activate
neighbor 18.2.2.2 send-community extended
neighbor 18.3.3.3 activate
neighbor 18.3.3.3 send-community extended
exit-address-family
```

The below configuration example is for BGP PIC with TDM PW:

```
pseudowire-class pseudowire1
encapsulation mpls
control-word
  no status control-plane route-watch
status peer topology dual-homed

! Interface CEM0/0/0
  cem
    xconnect 17.1.1.1 4101 encapsulation mpls pw-class pseudowire1
```

Example: ATM IMA Configuration

The following example shows how to add a T1/E1 interface to an ATM IMA group as a part of an ATM over MPLS pseudowire configuration. For more information about how to configure pseudowires, see Configuring Pseudowire, on page 221
This section displays a partial configuration intended to demonstrate a specific feature.

controller t1 4/0/0
ima-group 0
clock source line
interface atm4/0/ima0
pvc 1/33 l2transport
encapsulation aal0
xconnect 1.1.1.1 33 encapsulation mpls

Example: ATM over MPLS

The following sections contain sample ATM over MPLS configurations:

Cell Packing Configuration Examples

The following sections contain sample ATM over MPLS configuration using Cell Relay:

VC Mode

CE 1 Configuration

interface Gig4/3/0
no negotiation auto
load-interval 30
interface Gig4/3/0
ip address 20.1.1.1 255.255.255.0
interface ATM4/2/4
no shut
exit
!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2

CE 2 Configuration

interface Gig8/8
no negotiation auto
load-interval 30
interface Gig8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
no shut
!
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 20.1.1.2 255.255.255.255 50.1.1.1
PE 1 Configuration

interface Loopback0
ip address 192.168.37.3 255.255.255.255
!
interface ATM0/0/0
no shut
!
interface ATM0/0/0
atm mcpt-timers 150 1000 4095
interface ATM0/0/0.10 point
pvc 20/101 l2transport
encapsulation aal0
cell-packing 20 mcpt-timer 1
xconnect 192.168.37.2 100 encapsulation mpls
!
interface Gig0/3/0
no shut
ip address 40.1.1.1 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

PE 2 Configuration

interface Loopback0
ip address 192.168.37.2 255.255.255.255
!
interface ATM9/3/1
no shut
!
interface ATM9/3/1
atm mcpt-timers 150 1000 4095
interface ATM9/3/1.10 point
pvc 20/101 l2transport
encapsulation aal0
cell-packing 20 mcpt-timer 1
xconnect 192.168.37.3 100 encapsulation mpls
!
interface Gig6/2
no shut
ip address 40.1.1.2 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf
VP Mode

CE 1 Configuration

interface Gig4/3/0	no negotiation auto
load-interval 30
interface Gig4/3/0
ip address 20.1.1.1 255.255.255.0
interface ATM4/2/4
! interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
! ip route 30.1.1.2 255.255.255.255 50.1.1.2

CE 2 Configuration

! interface Gig8/8	no negotiation auto
load-interval 30
interface Gig8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
no shut
! interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
! ip route 20.1.1.2 255.255.255.255 50.1.1.1

PE 1 Configuration

interface Loopback0
ip address 192.168.37.3 255.255.255.255
! interface ATM0/0/0
no shut
! interface ATM0/0/0
atm mcpt-timers 150 1000 4095
interface ATM0/0/0.50 multipoint
atm pvp 20 12transport
cell-packing 10 mcpt-timer 1
xconnect 192.168.37.2 100 encapsulation mpls
! interface Gig0/3/0
no shut
ip address 40.1.1.1 255.255.0.0
mpls ip
! mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

PE 2 Configuration

! interface Loopback0
ip address 192.168.37.2 255.255.255.255
! interface ATM9/3/1
no shut
! interface ATM9/3/1
atm mcpt-timers 150 1000 4095
interface ATM9/3/1.50 multipoint
atm pvp 20 12transport
cell-packing 10 mcpt-timer 1
xconnect 192.168.37.3 100 encapsulation mpls
! interface Gig6/2
no shut
ip address 40.1.1.2 255.255.0.0
mpls ip
! mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

Cell Relay Configuration Examples

The following sections contain sample ATM over MPLS configuration using Cell Relay:

VC Mode

CE 1 Configuration

! interface gigabitethernet4/3/0
no negotiation auto
load-interval 30
interface gigabitethernet4/3/0
ip address 20.1.1.1 255.255.255.0
! interface ATM4/2/4
! interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
! ip route 30.1.1.2 255.255.255.255 50.1.1.2
CE 2 Configuration

interface gigabitethernet8/8
no negotiation auto
load-interval 30
interface gigabitethernet8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
!
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 20.1.1.2 255.255.255.255 50.1.1.1

PE 1 Configuration

!
interface Loopback0
ip address 192.168.37.3 255.255.255.255
!
interface ATM0/0/0
!
interface ATM0/0/0.10 point
pvc 20/101 l2transport
encapsulation aal0
xconnect 192.168.37.2 100 encapsulation mpls
!
interface gigabitethernet0/3/0
ip address 40.1.1.1 255.255.0.0
mpls ip
!
  mpls ip
  mpls label protocol ldp
  mpls ldp router-id Loopback0 force
  mpls ldp graceful-restart
  router ospf 1
  network 40.1.0.0 0.0.255.255 area 1
  network 192.168.37.0 0.0.0.255 area 1
  nsf

PE 2 Configuration

!
interface Loopback0
ip address 192.168.37.2 255.255.255.255
!
interface ATM9/3/1
!
interface ATM9/3/1.10 point
pvc 20/101 l2transport
encapsulation aal0
xconnect 192.168.37.3 100 encapsulation mpls
!
interface gigabitethernet6/2
ip address 40.1.1.2 255.255.0.0
mpls ip
!
  mpls ip
  mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1	nsf

VP Mode

CE 1 Configuration

!
interface gigabitethernet4/3/0
no negotiation auto
load-interval 30
interface gigabitethernet4/3/0
ip address 20.1.1.1 255.255.255.0
!
interface ATM4/2/4
!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2

CE 2 Configuration

!
interface gigabitethernet8/8
no negotiation auto
load-interval 30
interface gigabitethernet8/8
ip address 30.1.1.1 255.255.255.0
!
interface ATM6/2/1
!
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 20.1.1.2 255.255.255.255 50.1.1.1

PE 1 Configuration

interface Loopback0
ip address 192.168.37.3 255.255.255.255
!
interface ATM0/0/0
interface ATM0/0/0.50 multipoint
atm pvp 20 l2transport
xconnect 192.168.37.2 100 encapsulation mpls
!
interface gigabitethernet0/3/0
ip address 40.1.1.1 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

PE 2 Configuration

interface Loopback0
ip address 192.168.37.2 255.255.255.255
!
!
interface ATM9/3/1
interface ATM9/3/1.50 multipoint
atm pvp 20 l2transport
xconnect 192.168.37.3 100 encapsulation mpls
!
interface gigabitethernet6/2
ip address 40.1.1.2 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

Example: Ethernet over MPLS

PE 1 Configuration

!
mpls label range 16 12000 static 12001 16000
mpls label protocol ldp
mpls ldp neighbor 10.1.1.1 targeted ldp
mpls ldp graceful-restart
multilink bundle-name authenticated
!
!
!
redundancy
mode sso
!
!
ip tftp source-interface GigabitEthernet0
!
interface Loopback0
ip address 10.5.5.5 255.255.255.255
!
interface GigabitEthernet0/0/4
no ip address
negotiation auto
!

service instance 2 ethernet
   encapsulation dot1q 2
   xconnect 10.1.1.1 1001 encapsulation mpls
!

service instance 3 ethernet
   encapsulation dot1q 3
   xconnect 10.1.1.1 1002 encapsulation mpls
!

! interface GigabitEthernet0/0/5
   ip address 172.7.7.77 255.0.0.0
   negotiation auto
   mpls ip
   mpls label protocol ldp
!

router ospf 1
  router-id 5.5.5.5
  network 5.5.5.5 0.0.0.0 area 0
  network 172.0.0.0 0.255.255.255 area 0
  network 10.33.33.33 0.0.0.0 area 0
  network 192.0.0.0 0.255.255.255 area 0
!

PE 2 Configuration
!
  mpls label range 16 12000 static 12001 16000
  mpls label protocol ldp
  mpls ldp neighbor 10.5.5.5 targeted ldp
  mpls ldp graceful-restart
  multilink bundle-name authenticated
!
  redundancy
  mode sso
!
  !
  ip tftp source-interface GigabitEthernet0
!

! interface Loopback0
  ip address 10.1.1.1 255.255.255.255
!

interface GigabitEthernet0/0/4
  no ip address
  negotiation auto
!

service instance 2 ethernet
   encapsulation dot1q 2
   xconnect 10.5.5.5 1001 encapsulation mpls
!

service instance 3 ethernet
   encapsulation dot1q 3
   xconnect 10.5.5.5 1002 encapsulation mpls
!

! interface GigabitEthernet0/0/5
  ip address 172.7.7.7 255.0.0.0
  negotiation auto
  mpls ip
mpls label protocol ldp
!
router ospf 1
 router-id 10.1.1.1
 network 10.1.1.1 0.0.0.0 area 0
 network 172.0.0.0 0.255.255.255 area 0
 network 10.33.33.33 0.0.0.0 area 0
 network 192.0.0.0 0.255.255.255 area 0
!

Example: Ethernet over MPLS
Example: Ethernet over MPLS
# Digital Optical Monitoring for Transceivers

Starting with release Cisco IOS XE Release 3.13, Digital Optical Monitoring (DOM) is supported for the SFP, SFP+, and XFP transceiver modules.

DOM is supported for ASR 900 RSP3 Module.


For a list of modules, see [Cisco ASR 903 Series Aggregation Services Router Hardware Installation Guide](#).

Real time DOM data is collected from SFPs, SFP+, and XFPs periodically and compared with warning and alarm threshold table values.

The DOM data collected are transceiver transmit bias current, transceiver transmit power, transceiver receive power, and transceiver power supply voltage.

The syslog messages are displayed when alarm threshold values are crossed.

---

**Note**

The transceiver parameters are not monitored when the port is in ADMIN-DOWN.
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 that support 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 Cisco ASR 903 Series Router.

- Understanding Synchronous Ethernet ESMC and SSM, on page 277
- Restrictions and Usage Guidelines, on page 279
- Configuring Synchronous Ethernet ESMC and SSM, on page 279
- Managing Clock Source Selection, on page 283
- Verifying the Configuration, on page 285
- Troubleshooting, on page 285
- Configuration Examples, on page 287
- SSM Support on Cisco ASR 900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 Interface Module, on page 287
- SSM Support on Cisco 48-Port T3/E3 CEM Interface Module, on page 289

Understanding Synchronous Ethernet ESMC and SSM

Ethernet Synchronization Message Channel (ESMC) 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, 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 Cisco ASR 903 Series Router synchronizes to the best available clock source. If no better clock sources are available, the router remains synchronized to the current clock source.

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

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

Conversely, PTP clock sources are not supported with synchronous Ethernet. However, you can use hybrid clocking to allow the router to obtain frequency using Synchronous Ethernet and phase using PTP.

Clock Selection Modes

The Cisco ASR 903 Series Router supports two clock selection modes, which are described in the following sections.

QL-Enabled Mode

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

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

QL-Disabled Mode

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

- Clock availability
- Priority

You can use override the default clock selection using the commands described in the Managing Clock Source Selection, on page 283.

8275.1 profile does not support QL-disabled mode on RSP3.

Managing Clock Selection

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

- Hold-Off Time: If a clock source goes down, the router 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 router 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 283.

Restrictions and Usage Guidelines

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

• To use the `network-clock synchronization ssm option` command, ensure that the router 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 router goes into hold-over mode during switchover and restarts clock selection when the switchover is complete.

• 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.

• Copper SFP is not supported for SyncE Rx and Tx on the uplink interfaces. SyncE Rx and Tx is supported on the uplink interfaces only for fiber SFP only.

Configuring Synchronous Ethernet ESMC and SSM

Follow these steps to configure ESMC and SSM on the Cisco ASR 903 Series 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. network-clock input-source priority {interface interface_name slot/card/port | ptp domain domain_num | {external {R0 | R1 | { t1 | sf | esf } linecode {ami | b8zs} line-build-out length} | e1 | crc4 | fas} [125ohm | 75ohm] linecode [hdb3 | ami] | 10m}}
7. network-clock synchronization mode ql-enabled
8. network-clock hold-off {0 | milliseconds} global
9. network-clock wait-to-restore seconds global
10. network-clock revertive
### 11. esmc process

### 12. network-clock external \{\text{r0} / \text{r1} \} hold-off \{0 \mid \text{milliseconds}\}

### 13. network-clock quality-level \{\text{tx} \mid \text{rx}\} value \{\text{interface} \text{ interface-name slot/card/port} \mid \text{controller} \{\text{E1} \mid \text{BITS}\} \text{ slot/card/port} \mid \text{external} \{2\text{m} \mid 10\text{m}\}\}

### 14. interface type number

### 15. synchronous mode

### 16. esmc mode [ql-disabled \mid \text{tx} \mid \text{rx}] value

### 17. network-clock hold-off \{0 \mid \text{milliseconds}\}

### 18. network-clock wait-to-restore seconds

### 19. 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>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
</tbody>
</table>

| **Step 2** | configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal | |

| **Step 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 | |
| **Note:** | This command must be configured before any input source. |

| **Step 4** | network-clock eec \{1 \mid 2\} | Specifies the Ethernet Equipment Clock (EEC) type. Valid values are |
| **Example:** | Router(config)# network-clock eec 1 | |
| **Option 1:** | ITU-T G.8262 option 1 (2048) |
| **Option 2:** | ITU-T G.8262 option 2 and Telcordia GR-1244 (1544) |

<p>| <strong>Step 5</strong> | network-clock synchronization ssm option {1 \mid 2 \mid \text{GEN1} \mid \text{GEN2}} | Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command: |
| <strong>Example:</strong> | Router(config)# network-clock synchronization ssm option 2 GEN2 | |
| <strong>Option 1:</strong> | refers to G.781 synchronization option 1, which is designed for Europe. This is the default value. |
| <strong>Option 2:</strong> | refers to G.781 synchronization option 2, which is designed for the United States. |
| <strong>GEN1:</strong> | specifies option 2 Generation 1 synchronization. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• GEN2 specifies option 2 Generation 2 synchronization.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Enables you to select an interface as an input clock for the router. You can select the BITS, Gigabit Ethernet 0/0, Gigabit Ethernet 0/1 interfaces, or GPS interfaces, or an external interface.</td>
</tr>
<tr>
<td>network-clock input-source priority {interface interface_name slot/card/port</td>
<td>ptp domain domain_num</td>
</tr>
<tr>
<td>Example: Router(config)# network-clock input-source 1 interface GigabitEthernet 0/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Before configuring ethernet intreface as clock source, you should configure synchronous mode under interface configuration.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enables automatic selection of a clock source based on quality level (QL).</td>
</tr>
<tr>
<td>network-clock synchronization mode ql-enabled</td>
<td></td>
</tr>
<tr>
<td>Example: Router(config)# network-clock synchronization mode ql-enabled</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This command is disabled by default.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>(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.</td>
</tr>
<tr>
<td>network-clock hold-off {0</td>
<td>milliseconds} global</td>
</tr>
<tr>
<td>Example: Router(config)# network-clock hold-off 0 global</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can also specify a hold-off value for an individual interface using the network-clock hold-off command in interface mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>(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.</td>
</tr>
<tr>
<td>network-clock wait-to-restore seconds global</td>
<td></td>
</tr>
<tr>
<td>Example: Router(config)# network-clock wait-to-restore 70 global</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can also specify a wait-to-restore value for an individual interface using the network-clock wait-to-restore command in interface mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>(Optional) Sets the router in revertive switching mode when recovering from a failure. To disable revertive mode, use the no form of this command.</td>
</tr>
<tr>
<td>network-clock revertive</td>
<td></td>
</tr>
<tr>
<td>Example: Router(config)# network-clock revertive</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Enables the ESMC process globally.</td>
</tr>
<tr>
<td>esmc process</td>
<td></td>
</tr>
<tr>
<td>Example: Router(config)# esmc process</td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td>network-clock external ([r0 \mid r1]) hold-off (0 \mid \text{milliseconds})</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock external r0 hold-off 0</td>
</tr>
</tbody>
</table>

| Step 13 | network-clock quality-level \(\{\text{tx} \mid \text{rx}\}\) value \(\{\text{interface interface-name slot/card/port } \mid \text{controller [E1|BITS]} \mid \text{slot/card/port } \mid \text{external [2m|10m]}\}\) | Specifies a quality level for a line or external clock source. |
|---------|-------------------------------------------------|----------------------------------------------------------|
| Example: | Router(config)# network-clock quality-level rx ql-pRC external R0 e1 cas crc4 | The available quality values depend on the G.781 synchronization settings specified by the `network-clock synchronization ssm` option command: |
| | | • Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU. |
| | | • Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS. |
| | | • Option 2, GEN2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS. |

<table>
<thead>
<tr>
<th>Step 14</th>
<th>interface (\text{type number})</th>
<th>Enters interface configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</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>Example:</td>
<td>Router(config-if)# synchronous mode</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 16</th>
<th>esmc mode ([\text{ql-disabled} \mid \text{tx} \mid \text{rx}]) value</th>
<th>Enables the ESMC process at the interface level. The <code>no</code> form of the command disables the ESMC process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-if)# esmc mode rx QL-STU</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 17</th>
<th>network-clock hold-off ({0 \mid \text{milliseconds}})</th>
<th>(Optional) Configures an interface-specific hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-if)# network-clock hold-off 0</td>
<td>You can configure the hold-off time to either 0 or any value between 50 to 10000 ms. The default value is 300 ms.</td>
</tr>
</tbody>
</table>
Purpose
Command or Action

Step 18
network-clock wait-to-restore \textit{seconds}
Example:
\verbatim{Router(config-if)# network-clock wait-to-restore 70}

(Optional) Configures the wait-to-restore timer for an individual synchronous Ethernet interface.

Step 19
end
Example:
\verbatim{Router(config-if)# end}

Exits interface configuration mode and returns to privileged EXEC mode.

What to do next
You can use the \texttt{show network-clocks} command to verify your configuration.

Managing Clock Source Selection

The following sections describe how to manage the selection on the Cisco ASR 903 Series Router:

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 \texttt{network-clock switch manual} command in global configuration mode.

\textbf{Note}

The new clock source must be of higher quality than the current clock source; otherwise the router does not select the new clock source.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{network-clock switch manual external R0</td>
<td>R1}{E1</td>
</tr>
<tr>
<td>\verbatim{Router# network-clock switch manual external r0 e1 crc4 120ohms t0}</td>
<td></td>
</tr>
<tr>
<td>\texttt{network-clock clear switch {t0</td>
<td>external slot/card/port [10m</td>
</tr>
<tr>
<td>\verbatim{Router# network-clock clear switch t0}</td>
<td></td>
</tr>
</tbody>
</table>
Forcing a Clock Source Selection

To force the router 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>
</tbody>
</table>

Router# network-clock switch force r0 e1 crc4 120ohms t0

<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>
</tbody>
</table>

Router# network-clock clear switch t0

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>
</tbody>
</table>

Router# network-clock clear switch t0

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 router from selecting a specific synchronous Ethernet clock source, use the `network-clock set lockout` command in global configuration mode.
### 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} R0</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 your 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 router clock synchronization state.
- `show network-clock synchronization detail`—Displays the details of network clock synchronization parameters at the global and interface levels.

### Troubleshooting

Table 24: SyncE Debug Commands, on page 286 list the debug commands that are available for troubleshooting the SyncE configuration on the Cisco ASR 903 Series Router:
We recommend that you do not use `debug` commands without TAC supervision.

### Table 24: SyncE Debug Commands

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

### Table 25: Troubleshooting Scenarios

Table 25: Troubleshooting Scenarios, on page 286 provides the information about troubleshooting your configuration.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clock selection</strong></td>
<td>• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the nonrevertive configurations are in place.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Incorrect QL values</strong></td>
<td>• Ensure that there is no framing mismatch with the SSM option.</td>
</tr>
<tr>
<td></td>
<td>• Reproduce the issue using the debug network-clock errors and debug network-clock event commands.</td>
</tr>
<tr>
<td><strong>Alarms</strong></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Incorrect clock limit set or queue limit disabled mode</strong></td>
<td>• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>show network-clock synchronization</code> command to confirm if the system is in revertime mode or nonrevertive mode and verify the non-revertive configurations.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
Problem | Solution
--- | ---
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.

### Configuration Examples

**Example: Input Synchronous Ethernet Clocking**

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

```plaintext
! 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
```

**SSM Support on Cisco ASR900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 Interface Module**

SSM is carried over OC-3 and OC-12 optical links. Effective Cisco IOS-XE release 3.18 SP, the SSM is transported in the S1 byte when it is carried over an optical line for SONET and SDH. The SSM messages enable SONET and SDH devices to select the highest quality timing reference automatically and avoid the timing loops.

SSM is supported on Cisco ASR 900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 Module. It has four ports and the default rate is OC-3. OC-3 rate is supported on all the four ports and OC-12 rate is supported on first port only.
S1 Byte

The SSM is transported in the S1 byte when it is carried over an optical line for SONET and SDH. S1 byte resides in Multiplex Section Overhead (MSOH) in SDH frame. The last four bits (5 to 8) carries SSM information.

Supported Quality Levels

The quality levels supported for SDH framing mode are:

- QL-PRC
- QL-SSU-A
- QL-SSU-B
- QL-SEC (SDH equipment clock)
- QL-DNU

The quality levels supported for SONET framing mode are:

- GEN1—PRS, STU, ST2, ST3, SMC, ST4, and DUS
- GEN2—PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, and DUS

Configuring SSM on Cisco ASR 900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 IM

```
enable
configure terminal
network-clock synchronization automatic
network-clock eec 1
network-clock synchronization ssm option 2 GEN2
controller SONET 0/0/0
framing sdh
network-clock input-source 10 controller SONET 0/5/1
network-clock synchronization mode ql-enabled
network-clock hold-off 0
network-clock wait-to-restore 70
network-clock revertive
network-clock quality-level tx ql-prC controller SONET 0/0/0
network-clock quality-level rx ql-ssu-a controller SONET 0/5/1
network-clock hold-off 0 global
network-clock wait-to-restore 70
end
```

Configuring Clock Source

```
enable
configure terminal
controller sonet 0/5/0
clock source line
end
```
Verification of SSM Configuration

Use the `show network-clocks synchronization` command to verify the SSM configuration on Cisco ASR 900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 IM:

```
Router#show network-clocks synchronization
Symbols:   En - Enable, Dis - Disable, Adis - Admin Disable
          NA - Not Applicable
          * - Synchronization source selected
          # - Synchronization source force selected
          & - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : TenGigabitEthernet0/3/0
Hold-off (global) : 300 ms
Wait-to-restore (global) : 0 sec
Tsm Delay : 180 ms
Revertive : Yes

Nominated Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>SigType</th>
<th>Mode/QL</th>
<th>Prio</th>
<th>QL_IN</th>
<th>ESMC Tx</th>
<th>ESMC Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>NA</td>
<td>NA/Dis</td>
<td>251</td>
<td>QL-SEC</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>*SONET 0/5/1</td>
<td>NA</td>
<td>NA/En</td>
<td>10</td>
<td>QL-PRC</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

Router#
```

SSM Support on Cisco 48-Port T3/E3 CEM Interface Module

Synchronization Status Message (SSM) is transported over T3 links using proprietary method. SSM enables T3 to select the highest quality timing reference automatically and avoid the timing loops.

SSM is supported on Cisco 48-Port T3/E3 CEM Interface Module.

---

Note

Effective IOS XE Everest 16.5.1, E3 mode is not supported.

Supported Quality Levels

The quality levels supported on T3 are:

- GEN1—PRS, STU, ST2, ST3, SMC, ST4, and DUS
- GEN2—PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, and DUS

Configuring SSM on Cisco 48-Port T3/E3 CEM Interface Module

```
enable
configure terminal
controller media-type controller 0/5/0
mode t3
controller t3 0/0/0
```
network-clock synchronization automatic
network-clock eec 1
network-clock synchronization ssm option 2 GEN2
network-clock input-source i0 controller t3 0/5/1
network-clock synchronization mode ql-enabled
network-clock hold-off 0
network-clock wait-to-restore 70
network-clock revertive
network-clock quality-level tx ql-prs controller t3 0/0/0
network-clock quality-level rx ql-st2 controller t3 0/5/1
network-clock hold-off 0
network-clock wait-to-restore 70
end

Configuring Clock Source

  enable
  configure terminal
  controller media-type controller 0/5/0
  mode t3
  controller t3 0/5/0
  clock source line
  end

Verification of SSM Configuration

Use the `show network-clocks synchronization detail` command to verify the SSM configuration on Cisco 48-Port T3/E3 CEM Interface Module:

```plaintext
show network-clocks synchronization detail
Symbols: En - Enable, Dis - Disable, Adis - Admin Disable
NA - Not Applicable
* - Synchronization source selected
# - Synchronization source force selected
& - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 1544 (EEC-Option2)
Clock State : Frequency Locked
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : GEN1
T0 : T3 0/0/21
Hold-off (global) : 300 ms
Wait-to-restore (global) : 0 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 1
Squelch Threshold: QL-ST3
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (begin)-> 2A (ql_mode_enable)-> 1A (src_added)-> 1A (ql_change)->
  1A (sf_change)-> 1A (ql_change)-> 1A

Nominated Interfaces

  Interface SigType Mode/QL Prio QL_IN ESMC Tx ESMC Rx
  Internal NA NA/Dis 251 QL-ST3 NA NA
  *T3 0/0/21 NA NA/En 2 QL-PRS NA NA
```
Interface:
--------------------------------------------------
Local Interface: Internal
Signal Type: NA
Mode: NA(Q1-enabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 251
QL Receive: QL-ST3
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 0
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Active Alarms: None
Slot Disabled: FALSE
SNMP input source index: 1
SNMP parent list index: 0
Description: None

Local Interface: T3 0/0/21
Signal Type: NA
Mode: NA(Q1-enabled)
SSM Tx: ENABLED
SSM Rx: ENABLED
Priority: 2
QL Receive: QL-PRS
QL Receive Configured: QL-PRS
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Active Alarms: None
Slot Disabled: FALSE
SNMP input source index: 8
SNMP parent list index: 0
Description: None
Verification of SSM Configuration
CHAPTER 17

Configuring the SDM Template

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

- Prerequisites for the SDM Template, on page 293
- Restrictions for the SDM Template, on page 293
- Information About the SDM Template, on page 295
- Selecting the SDM Template, on page 306
- Verifying the SDM Template, on page 308
- SDM Template Supported Features on RSP3 Module, on page 308

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

- Do not configure CoPP and BDI-MTU SDM templates together, as it may result in a resource depletion on the device and can lead to a reload.

- If you do not enable the EFP feature template, then there is no traffic flow between EFP and VFI (when EFP is with Split Horizon group and VFI is default). But when you enable the EFP feature template, then there is traffic flow between EFP and VFI because of design limitations.

- You cannot edit individual values in a template category as all templates are predefined.

- You cannot use a new SDM template without reloading the router.

- SDM templates are supported only by the Metro Aggregation Services license. Use the help option of the sdm prefer command to display the supported SDM templates.

- A mismatch in an SDM template between an active RSP and standby RSP results in a reload of the standby RSP. During reload, SDM template of the standby RSP synchronizes with the SDM template of the active RSP.
Restrictions for the SDM Template

- To revert to the current SDM template after using the `sdm prefer` command (which initiates reload of a new SDM template), you must wait for the reload to complete.

- Using the `configure replace` command which results in changes in the current SDM template is not supported.

- The supported group numbers are for scaling in uni-dimension. When scaling in multidimension, the numbers can vary as certain features may share resources.

- When scaling, features using Multiprotocol Label Switching (MPLS) are limited by the number of MPLS labels.

- Internal TCAM usage that is reserved for IPv6 is 133-135 entries. TCAM space that is allotted for SDM template is 135 entries on the router.

- EAID Exhaust occurs when two paths are MPLS and two are IP. It does not occur if all the four paths are IP.

- The following restrictions apply to the maximum IPv6 QoS ACL SDM template:
  - The number of QoS ACL class maps and policy maps that are supported depends on the maximum TCAM entries available.
  - The software solution with expansion is applicable only for maximum QoS SDM template and more than eight Layer 4-port matches are supported for the maximum QoS SDM template. For other templates, due to hardware restriction, a maximum of eight Layer 4-port operators is supported per interface.
  - Ethernet CFM, Ethernet OAM, and Y.1731 protocols are not supported. Features dependent on these protocols are impacted.
  - Layer 2 monitoring features are not supported.
  - The S-TAG based fields are not supported for classification, if IPv6 address match exists in the policy-map.
  - Only eight Layer 4 operations are supported in templates other than maximum IPv6 QoS ACL template.

<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>

Note: These times are for the Activity Time Release Reload to SSObulkSync state.
Information About the SDM Template

The SDM templates are used to optimize system resources in the router to support specific features, depending on how the router is used in the network. The SDM templates allocate Ternary Content Addressable Memory (TCAM) resources to support different features. You can select the default template to balance system resources or select specific templates to support the required features.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP3.

*Table 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>192k (ipv4 routes + mpls labels)</td>
<td>76k (ipv4 routes + mpls labels)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MPLS Labels = 32000</td>
<td>MPLS Labels = 32000</td>
</tr>
<tr>
<td>IPv6/VPNv6 Routes</td>
<td>8192</td>
<td>8192</td>
<td>65536</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 configurable)</td>
<td>1000 (984 user configurable)</td>
<td>1000 (984 user configurable)</td>
</tr>
<tr>
<td>IPv6 ACL entries</td>
<td>128 (124 user configurable)</td>
<td>128 (124 user configurable)</td>
<td>128 (124 user configurable)</td>
</tr>
<tr>
<td>v4 QOS Classifications</td>
<td>16000</td>
<td>16000</td>
<td>16000</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>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>Maximum Policer counters per ASIC/system</td>
<td>12000/24000</td>
<td>12000/24000</td>
<td>12000/24000</td>
</tr>
</tbody>
</table>

Cisco ASR 900 Router Series Configuration Guide, Cisco IOS XE Release 3S
### 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 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>
<tr>
<td>Max number IEEE 802.1ag/Y.1731(CFM) instances at 1sec for xconnect</td>
<td>1000</td>
<td>1000</td>
<td>1000</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 3.3 ms for BD &amp; xconenct</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 IEEE 802.1ag/Y.1731(CFM) instances at 1Sec for BD</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 3.3ms</td>
<td>1023</td>
<td>1023</td>
<td>1023</td>
</tr>
<tr>
<td>Max number of BFD sessions at 100ms</td>
<td>1023</td>
<td>1023</td>
<td>1023</td>
</tr>
<tr>
<td>Max number of BFD sessions at 1S</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>Ingress Qos TCAM</td>
<td>4000</td>
<td>4000</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Egress Qos TCAM</td>
<td>5000</td>
<td>5000</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>IPv6 ACL TCAM</td>
<td>1000</td>
<td>1000</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>ACL TCAM</td>
<td>4000</td>
<td>2000</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Max-QoS-Video</td>
<td>4000</td>
<td>1000</td>
<td>1000</td>
<td>NA</td>
</tr>
<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)</td>
<td>4000</td>
<td>4000</td>
<td>65536</td>
<td>4000</td>
</tr>
<tr>
<td>mapping</td>
<td></td>
<td></td>
<td></td>
<td></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)</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>lite</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>instances</td>
<td></td>
<td></td>
<td></td>
<td></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>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>Queues per Application-Specific Integrated Circuit (ASIC)</td>
<td>4095</td>
<td>4095</td>
<td>4095</td>
<td>4095</td>
</tr>
<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>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 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>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)</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>
</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>Default Template</th>
<th>Video Template</th>
<th>IP Template</th>
<th>Maximum IPv6 QoS Template</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>IPv6 ACL</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td>IPv6 QoS classification</td>
<td>4096</td>
<td>4096</td>
<td>4096</td>
<td>4096</td>
</tr>
<tr>
<td>Maximum Number of Layer 4 Source/Destination matches per interface</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>NA</td>
</tr>
</tbody>
</table>

5 Using IPv4 and VPNv4 routes concurrently reduces the maximum scaled value as both the routes use the same TCAM space.

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

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

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

9 User available queues are 1920.

10 TCAM consumption for IPv6 Qos ACL Layer 4 port match operations increase with Maximum IPv6 Qos SDM template.
<table>
<thead>
<tr>
<th>Resource</th>
<th>IP template</th>
<th>Video template</th>
</tr>
</thead>
<tbody>
<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>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</td>
<td>2000</td>
<td>4000</td>
</tr>
<tr>
<td>Queues per Application-Specific Integrated Circuit (ASIC)</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>
</tbody>
</table>
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>
</tbody>
</table>

11. Using IPv4 and VPNv4 routes concurrently reduces the maximum scaled value as both the routes use the same TCAM space.
12. User available routes are 3967.
13. Due to label space limitation of 16000 VPNv4 routes, to achieve 24000 VPNv4 routes in IP template use per VRF mode.
14. Using Layer 2 and Layer 3 multicast groups concurrently reduces the scale number to 1947.
15. ACLs contend for TCAM resources with Multicast Virtual Private Network (MVPN).
16. User available queues are 1920.
### Information About the SDM Template

<table>
<thead>
<tr>
<th>Resource</th>
<th>VPNv4/v6 template</th>
<th>Video template</th>
</tr>
</thead>
<tbody>
<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 addresses</td>
<td>256000</td>
<td>256000</td>
</tr>
<tr>
<td>EFPS per BD</td>
<td>62</td>
<td>62</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>80000</td>
<td>80000</td>
</tr>
<tr>
<td>IPv6 routes</td>
<td>40000</td>
<td>8000</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[^17]</td>
<td>2000</td>
<td>8000</td>
</tr>
<tr>
<td>IPv6 routing groups[^18]</td>
<td>2000</td>
<td>8000</td>
</tr>
<tr>
<td>IPv4 multicast groups[^19]</td>
<td>2000</td>
<td>10000</td>
</tr>
<tr>
<td>IPv6 multicast groups[^20]</td>
<td>2000</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>8000</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>
</tbody>
</table>
### Selecting the SDM Template

Overall multicast groups in video template can be scaled to 8000 individually or in combination with other multicast features. For example: IPv4 routing groups can be scaled to 8000 or IPv4 routing groups and IPv6 routing groups together can be scaled to 8000.

---

**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}`

---

<table>
<thead>
<tr>
<th>Resource</th>
<th>VPNv4/v6 template</th>
<th>Video template</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELM1 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>
<tr>
<td>FRR TE midpoints</td>
<td>7000</td>
<td>7000</td>
</tr>
<tr>
<td>STP instances</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>BFD sessions</td>
<td>511</td>
<td>511</td>
</tr>
<tr>
<td>HSRP VRRP sessions</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Maximum EC groups</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Maximum interfaces per EC groups</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Maximum SPAN RSPAN sessions</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>IPv4 tunnel entries</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum VPNv4 and VPNv6 pre-fixes</td>
<td>64000</td>
<td>64000</td>
</tr>
</tbody>
</table>

---

17 Overall multicast groups in video template can be scaled to 8000 individually or in combination with other multicast features. For example: IPv4 routing groups can be scaled to 8000 or IPv4 routing groups and IPv6 routing groups together can be scaled to 8000.

18 See footnote 7.

19 See footnote 7.

20 See footnote 7.

21 VPNv4 and VPNv6 together can be scaled up to 64000 in per-prefix mode.
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **enable** | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| Example: | Router> enable | |
| **Step 2** | **configure terminal** | Enters global configuration mode. |
| Example: | Router# configure terminal | |
| **Step 3** | **sdm prefer {default | video | ip | 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}** | Specifies the SDM template to be used on the router.  
- **default**—Balances all functions.  
- **video**—Increases multicast routes and ACLs.  
- **ip**—Increases IPv4/VPNv4 routes. This option is available only on RSP1A.  
- **mvpn_rsp1a**—Supports MVPN. This option is available only on RSP1A.  
- **VPNv4/v6**—Increases IPv4/VPNv4 routes. This option is available only on RSP1B.  
- **max-ipv6-acl**—Supports IPv6 QoS ACL routes. The NEQ Layer 4 operation is supported in maximum IPv6 QoS ACL template.  
  The maximum IPv6 QoS ACL template works in metro IP services license for RSP2.  
- **ipv4**—Enables the IPv4 template. This is supported on the RSP3 module.  
- **ipv6**—Enables the IPv6 feature template. This is supported on the RSP3 module.  
- **efp_feat_ext**—Enables the EFP feature template. This is supported on the RSP3 module.  
- **enable_8k_efp**—Enables the 8K EFP feature template. This is supported on the RSP3 module.  
- **enable_copp**—Enables the COPP feature template. This is supported on the RSP3 module.  
- **enable_l3vpn_cm**—Enables the L3VPN conditional marking feature template. This is supported on the RSP3 module.  
- **enable_match_inner_dscp**—Enables the match inner dscp feature template. This is supported on the RSP3 module. |
| Example: | Router(config)# sdm prefer default | |
### 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 30: SDM Templates and Supported Features

<table>
<thead>
<tr>
<th>SDM Template</th>
<th>Supported Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>sdm prefer vpls_stats_enable</td>
<td>VPLS Statistics</td>
</tr>
<tr>
<td>sdm prefer efp_feat_ext</td>
<td>Split-Horizon Groups</td>
</tr>
<tr>
<td>sdm prefer enable_8k_efp</td>
<td>8K EFP (4 Queue Model)</td>
</tr>
<tr>
<td>sdm prefer enable_match_inner_dscp</td>
<td>Match Inner DSCP</td>
</tr>
<tr>
<td>sdm prefer enable_copp</td>
<td>Control Plane Policing</td>
</tr>
</tbody>
</table>
### SDM Template

<table>
<thead>
<tr>
<th>SDM Template</th>
<th>Supported Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>sdm prefer enable_portchannel_qos_multiple_active</td>
<td>QoS Support on Port Channel LACP Active Active</td>
</tr>
<tr>
<td></td>
<td>16K EFP Support on Port Channel</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:

```plaintext
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:

```plaintext
router# show mpls l2transport vc 2200 detail
```

Local interface: Gi0/14/2 up, line protocol up, Ethernet:100 up
Destination address: 10.163.123.218, VC ID: 2200, VC status: up
Output interface: Te0/7/2, imposed label stack {24022 24025}
Preferred path: not configured
Default path: active
Next hop: 10.163.122.74
Create time: 20:31:49, last status change time: 16:27:32
Last label FSM state change time: 16:27:44
Signaling protocol: LDP, peer 10.163.123.218:0 up
Targeted Hello: 10.163.123.215 (LDP ID) -> 10.163.123.218, LDP is UP
Graceful restart: configured and enabled
Non stop routing: configured and enabled
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 110, remote 24025
Group ID: local 40, remote 67109248
MTU: local 9000, remote 9000
Remote interface description: TenGigE0_0_2_3.2200
Sequencing: receive disabled, send disabled
Control Word: Off (configured: autosense)
SSO Descriptor: 10.163.123.218/2200, local label: 110
Dataplane:
SSM segment/switch IDs: 16911/90633 (used), PWID: 71
VC statistics:
transit packet totals: receive 100, send 200
transit byte totals: receive 12800, send 25600
transit packet drops: receive 0, seq error 0, send 0

Split Horizon Enhancements on the RSP3 Module

Starting with Cisco IOS XE Release 16.6.1, the `efp_feat_ext` template is introduced. This template when enabled allows configuration of two split-horizon groups on the EVC bridge-domain.

- Two Split-horizon groups—Group 0 and Group 1 are configured through using the `bridge-domain bd number split-horizon group 0-1` command.

Prerequisites for Split-Horizon Groups on the RSP3 Module

- The `efp_feat_ext` template must be configured to enable the feature.
- Metro services license must be enabled; `LICENSE_ACTIVE_LEVEL=metroaggrservices,all:ASR-903;`

Restrictions for Split-Horizon Groups on the RSP3 Module

- 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 receive traffic from each other.
- We do not recommend 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 behaviour of split-horizon groups:

- Changing the split-horizon group on any EFP, results in traffic flooding back to same EFP for few milliseconds.
- A small traffic leak may be observed on defaulting an interface with higher number of EFP with split-horizon configured.
- BFD flaps and underlying IGP flaps may be observed upon changing split-horizon groups, if BFD is hardware based.

### Split-Horizon Supported Scale

8K EFPs are supported across RSP3-400 and 4K EFPs on RSP3-200.

<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.

### 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, \* 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 Model

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)#sdm prefer enable_8k_efp

Template configuration has been modified. Save config and Reload? [yes/no]: yes
Building configuration...

Jul 22 05:58:30.774 IST: Changes to the EFP template preferences have been stored[OK]
Proceeding with system reload...
Reload scheduled for 06:00:38 IST Fri Jul 22 2016 (in 2 minutes) by console
Reload reason: EFP template change

**Verifying 8K EFP Template**

You can verify the current template as below.

Device#sh sdm prefer current

The current sdm template is "default" template and efp template is "enable_8k_efp" template

**Configuring QOS in 8K EFP Model**

Below is sample configuration to configure egress policy map when 4Q mode is enabled.

Device#enable
Device#configure terminal
Device(config)#interface GigabitEthernet0/3/0
Device(config-if)#service instance 10 e
Device(config-if-srv)#service-policy output egress

Current configuration : 193 bytes
!
policy-map egress
class qos2
  shape average 2000000
class qos3
  shape average 3000000
class qos4
  shape average 4000000
class class-default
  shape average 5000000
!
end

Device#sh run class-map qos2
Building configuration...
!
Current configuration : 54 bytes
!
class-map match-all qos2
match qos-group 2
!
end

Device#sh run class-map qos3
Building configuration...
!
Current configuration : 54 bytes
!
class-map match-all qos3
match qos-group 3
!
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 qos-default
shape average 5000000
end

Device# show 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
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.

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:

```plaintext
router>enable
router#configure terminal
router(config)#sdm prefer enable_portchannel_qos_multiple_active
router(config)#platform port-channel 10 members-asic-id I
router(config)#platform qos-port-channel_multiple_active port-channel 10
router(config)#interface port-channel 10
router(config-if)#end
```

After the SDM template update, the device reloads automatically and you need to enter `yes` to save the configuration.

Verifying 16k EFP on Port Channel

The following are examples to verify for 16K EFP configuration on port channel.

```plaintext
Router# show etherchannel summary
Flags:  D - down P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3     S - Layer2
        U - in use     f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group  Port-channel  Protocol  Ports
-------+-----------------+-----------+-----------------------------------------------
10     Po10(RU)     LACP     Te0/5/0(bndl) Te0/5/1(bndl)

RU = L3 port-channel UP State
SU = L2 port-channel UP state
P/bndl = Bundled
S/susp = Suspended

Router# show ethernet service instance id interface stats
Port maximum number of service instances: 16000
Service Instance 12000, 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**

- Ingress and Egress marking are not supported.
• Egress COPP is not supported. COPP with marking is not supported.
• CPU bound traffic (punted traffic) flows is supported via the same queue with or without CoPP.
• Only match on access group is supported on a CoPP policy.
• Hierarchical policy is not supported with CoPP.
• Class-default is not supported on CoPP policy.
• User defined ACLs are not subjected to CoPP classified traffic.
• A CoPP policy map applied on a physical interface is functional.
• When COPP template is enabled, classification on outer Vlan, inner Vlan, Inner Vlan Cos, destination MAC address, source IP address, and destination IP address are not supported.

The template-based model is used to enable COPP features and disable some of the above mentioned QOS classifications.
• When COPP-template is enabled, matchInnerDSCP-template functionality 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 copp-system-acl-tftp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any any eq 69</td>
<td></td>
</tr>
<tr>
<td>TELNET</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-telnet</td>
<td>NQ_CPU_CONTROL_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp any any eq telnet</td>
<td></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>NTP - Network Time Protocol</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-ntp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq ntp</td>
<td></td>
</tr>
<tr>
<td>FTP - File Transfer Protocol</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-ftp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp host any eq ftp</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</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq snmp</td>
<td></td>
</tr>
<tr>
<td>TACACS - Terminal Access Controller</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-tacacs</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>Access-Control System</td>
<td></td>
<td>permit tcp any tacacs</td>
<td></td>
</tr>
<tr>
<td>FTP-DATA</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-ftpdata</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp any eq 20</td>
<td></td>
</tr>
<tr>
<td>HTTP - Hypertext Transfer Protocol</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-http</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp any eq www</td>
<td></td>
</tr>
<tr>
<td>WCCP - Web Cache Communication Protocol</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-wccp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq 2048 eq 2048</td>
<td></td>
</tr>
<tr>
<td>SSH - Secure Shell</td>
<td>Port Match</td>
<td>IP access list ext copp-system-acl-ssh</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp any eq 22</td>
<td></td>
</tr>
<tr>
<td>ICMP - Internet Control Message Protocol</td>
<td>Protocol Match</td>
<td>IP access list copp-system-acl-icmp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit icmp any eq</td>
<td></td>
</tr>
<tr>
<td>DHCP - Dynamic Host Configuration Protocol</td>
<td>Port Match</td>
<td>IP access list copp-system-acl-dhcp</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq bootps</td>
<td></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>MPLS- OAM</td>
<td>Port Match</td>
<td>IP access list</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>copp-system-acl-mplsoam permit udp any eq 3503 any</td>
<td></td>
</tr>
<tr>
<td>LDP - Label Distribution Protocol</td>
<td>Port Match</td>
<td>IP access list</td>
<td>NQ_CPU_CFM_Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>copp-system-acl-ldp permit udp any eq 646 any eq 646</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit tcp any eq 646</td>
<td></td>
</tr>
<tr>
<td>RADIUS - Remote Authentication</td>
<td>Port Match</td>
<td>IP access list</td>
<td>NQ_CPU_HOST_Q</td>
</tr>
<tr>
<td>Dial In User Service</td>
<td></td>
<td>copp-system-radius permit udp any eq 1812</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq 1813</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq 1645</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq 1646</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq 1812 any</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permit udp any eq 1645 any</td>
<td></td>
</tr>
</tbody>
</table>

**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.

Router# show policy-map control-plane
Control Plane
Service-policy input: control-plane-in
Class-map: telnet-class (match-all)
10521 packets, 673344 bytes
5 minute offered rate 18000 bps, drop rate 15000 bps
Match: access-group 102
police: cir 64000 bps, bc 8000 bytes
conformed 1430 packets, 91520 bytes; actions:
transmit
exceeded 9091 packets, 581824 bytes; actions:
drop
conformed 2000 bps, exceeded 15000 bps
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any

The following command is used to verify the TCAM usage on the router.

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

Type Total Used Free
QoS TCAM 2048 2 2046
VOQs 49152 808 48344
QoS Policers 32768 2 32766
QoS Policer Profiles 1023 1 1022
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 0 32768
QoS Support on Port Channel LACP Active Active

Link Aggregation Control Protocol (LACP) supports the automatic creation of ether channels by exchanging LACP packets between LAN ports. Cisco IOS XE Everest 16.6.1 release introduces the support of QoS on port channel LACP active active mode. A maximum of eight member links form a port channel and thus the traffic is transported through the port channel. This feature is supported on Cisco RSP3 Module.

Benefits of QoS Support on Port Channel LACP Active Active

- This feature facilitates increased bandwidth.
- The feature supports load balancing.
- This features allows support on QoS on Port Channel with one or more active member links.

Restrictions for QoS Support on Port Channel Active Active

- Policy-map on member links is not supported.
- 100G ports and 40G ports cannot be a part of the port channel.
- Total number of port channel bandwidth supported on a given ASIC should not exceed 80G.
- This feature is not supported on multicast traffic.
- Only 3k service instance (EFP) scale is supported on port channel active active.

Configuring QoS Support on Port Channel Active Active

Enabling Port Channel Active/Active

Use the following commands to enable port channel active active:

```bash
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:

```bash
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:

```bash
enable
configure terminal
```
Creating Port Channel Interface

Use the following commands to configure the port channel interface:

```conf
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:

```conf
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:

```conf
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:

```conf
enable
configure terminal
interface port-channel 10
service-policy output policymapqos
end
```
d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Po10(RU)</td>
<td>LACP</td>
<td>Te0/4/0(bndl)</td>
</tr>
</tbody>
</table>

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/ 10240000 bytes
(queue depth/total drops/no-buffer drops) 0/821727/0
(pktks 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/ 10240000 bytes
(queue depth/total drops/no-buffer drops) 0/440370/0
(pktks 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
(pktks output/bytes output) 1565/118342
```

Use the commands below to verify the configuration after enabling port channel active/active mode:

```
#show sdm prefer current
The current sdm template is "default"
The current portchannel template is "enable_portchannel_qos_multiple_active"
```
Match Inner DSCP on RSP3 Module

Starting with Cisco IOS XE Release 16.6.1, the match inner dscp template is introduced. This template allows DSCP policy map configuration on the RSP3 module for MPLS and tunnel terminated traffic.

Restrictions for Match Inner DSCP on RSP3 Module

- The IPv4 DSCP policy map configuration is not preserved in case of protection scenarios, where either primary or backup path is plane IP path and backup or primary is MPLS label path.
- Match on Inner DSCP for IPv6 is not supported.
- Only 1024 entries IPv4 TCAM entries are available. Hence, optimized usage of classes is recommended for configuration when policy map is applied on port channel or port or EFP.
- To support match on Inner DSCP for IPv4 when packets have MPLS forwarding type, three TCAM entries are added whenever there is a class map with match DSCP is configured.

One match is for normal DSCP scenario, one entry for Inner DSCP when outer header is MPLS header and other entry is when there is tunnel termination.

In Split Horizon template, each match DSCP class consumes 3 TCAM entries. For non-Split Horizon template, TCAM entries are one. For Class default, number of entries consumed is one. For TEFP, six entries are required for each match DSCP Class Map and two for class default.

Note
Some of the IPv4 qualifiers are not supported when Split Horizon template is configured as there are limitation of Copy Engines in IPv4 Resource database. Whenever Split Horizon template is enabled, four new qualifiers are added in IPV4 QoS Field Group.

Configuring Match Inner DSCP on RSP3 Module

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

Verifying Match Inner DSCP on RSP3 Module

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

<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 Policer 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>
Chapter 18

Tracing and Trace Management

This chapter contains the following sections:

- Tracing Overview, on page 327
- How Tracing Works, on page 328
- Tracing Levels, on page 328
- Viewing a Tracing Level, on page 329
- Setting a Tracing Level, on page 331
- Viewing the Content of the Trace Buffer, on page 331

Tracing Overview

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

---

Note

Starting release Cisco IOS XE Release 3.14 and later, logs are stored in compressed format.

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 tracelog directory. Trace files can be erased from this directory to recover space on the file system without impacting system performance.

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

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

Tracing cannot be disabled on the chassis. Trace levels, however, which set the message types that generate trace output, are user-configurable and can be set using the `set platform software trace` command. If a user wants to modify the trace level to increase or decrease the amount of trace message output, the user should set a new tracing level using the `set platform software trace` command. Trace levels can be set by process using the `all-modules` keyword within the `set platform software trace` command, or by module within a process. See the `set platform software trace` command reference for more information on this command, and the Tracing Levels, on page 328 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 32: Tracing Levels and Descriptions, on page 328 shows all of the trace levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

Table 32: 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>Trace Level</td>
<td>Level Number</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Verbose</td>
<td>8</td>
<td>All possible tracing messages are sent.</td>
</tr>
<tr>
<td>Noise</td>
<td>-</td>
<td>All possible trace messages for the module are logged. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.</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
```
### Viewing a Tracing Level

<table>
<thead>
<tr>
<th>Module</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>bsignal</td>
<td>Notice</td>
</tr>
<tr>
<td>btrace</td>
<td>Notice</td>
</tr>
<tr>
<td>cce</td>
<td>Notice</td>
</tr>
<tr>
<td>cdllib</td>
<td>Notice</td>
</tr>
<tr>
<td>cef</td>
<td>Notice</td>
</tr>
<tr>
<td>chasfs</td>
<td>Notice</td>
</tr>
<tr>
<td>chasutil</td>
<td>Notice</td>
</tr>
<tr>
<td>erspan</td>
<td>Notice</td>
</tr>
<tr>
<td>ess</td>
<td>Notice</td>
</tr>
<tr>
<td>ether-channel</td>
<td>Notice</td>
</tr>
<tr>
<td>evlib</td>
<td>Notice</td>
</tr>
<tr>
<td>evutil</td>
<td>Notice</td>
</tr>
<tr>
<td>file_alloc</td>
<td>Notice</td>
</tr>
<tr>
<td>fman_rp</td>
<td>Notice</td>
</tr>
<tr>
<td>fps</td>
<td>Notice</td>
</tr>
<tr>
<td>fw</td>
<td>Notice</td>
</tr>
<tr>
<td>icmp</td>
<td>Notice</td>
</tr>
<tr>
<td>interfaces</td>
<td>Notice</td>
</tr>
<tr>
<td>iosd</td>
<td>Notice</td>
</tr>
<tr>
<td>ipc</td>
<td>Notice</td>
</tr>
<tr>
<td>ipclog</td>
<td>Notice</td>
</tr>
<tr>
<td>iphc</td>
<td>Notice</td>
</tr>
<tr>
<td>ipsec</td>
<td>Notice</td>
</tr>
<tr>
<td>mgmte-acl</td>
<td>Notice</td>
</tr>
<tr>
<td>mlp</td>
<td>Notice</td>
</tr>
<tr>
<td>mqipc</td>
<td>Notice</td>
</tr>
<tr>
<td>nat</td>
<td>Notice</td>
</tr>
<tr>
<td>nbar</td>
<td>Notice</td>
</tr>
<tr>
<td>netflow</td>
<td>Notice</td>
</tr>
<tr>
<td>om</td>
<td>Notice</td>
</tr>
<tr>
<td>peer</td>
<td>Notice</td>
</tr>
<tr>
<td>qos</td>
<td>Notice</td>
</tr>
<tr>
<td>route-map</td>
<td>Notice</td>
</tr>
<tr>
<td>sbc</td>
<td>Notice</td>
</tr>
<tr>
<td>services</td>
<td>Notice</td>
</tr>
<tr>
<td>sw_wdog</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_acl_config_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_acl_db_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_cdlcore_message</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_cef_config_common_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_cef_config_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_dpdlb_config_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_fman_rp_comm_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_fman_rp_message</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_fw_config_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_hapi_tdl_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_icmp_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_ip_options_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_ipc_ack_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_ipsec_db_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_mcp_comm_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_mlp_config_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_mlp_db_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_om_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_ui_message</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_ui_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_urpf_config_type</td>
<td>Notice</td>
</tr>
<tr>
<td>tdlllib</td>
<td>Notice</td>
</tr>
<tr>
<td>trans_avl</td>
<td>Notice</td>
</tr>
<tr>
<td>uihandler</td>
<td>Notice</td>
</tr>
<tr>
<td>uipере</td>
<td>Notice</td>
</tr>
<tr>
<td>uistatus</td>
<td>Notice</td>
</tr>
<tr>
<td>urpf</td>
<td>Notice</td>
</tr>
</tbody>
</table>
Setting a Tracing Level

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

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

```
set platform software trace forwarding-manager F0 acl info
```

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

Viewing the Content of the Trace Buffer

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

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

```
Router# show platform software trace message host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in slot 0
```
CHAPTER 19

Configuring and Monitoring Alarm

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

This chapter includes the following sections:

- Monitoring Alarms, on page 333
- Configuring External Alarm Trigger, on page 338
- Alarm Filtering Support, on page 341

Monitoring Alarms

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

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

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

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

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

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

---

**Note**

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

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

Enabling the Logging Alarm Command

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

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

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

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

Examples of Alarm Messages

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

**SPA REMOVED**

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

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

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

**SPA RE-INSERTED**

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

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

**ALARMS for Router**

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

SPA Removed
Router# show facility-alarm status
System Totals Critical: 22 Major: 0 Minor: 0

<table>
<thead>
<tr>
<th>Source</th>
<th>Time</th>
<th>Severity</th>
<th>Description [Index]</th>
</tr>
</thead>
<tbody>
<tr>
<td>subslot 0/0</td>
<td>May 18 2016 14:50:49</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR [0]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/1</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/2</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/6</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/7</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/2/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/2/3</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/2/4</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/2/5</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/2/6</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>SONET 0/3/0</td>
<td>May 11 2016 18:54:25</td>
<td>INFO</td>
<td>Physical Port Administrative State Down [36]</td>
</tr>
<tr>
<td>xcvr container 0/3/1</td>
<td>May 11 2016 18:53:44</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/3/2</td>
<td>May 11 2016 18:53:44</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/3/3</td>
<td>May 11 2016 18:53:44</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/4/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/4/1</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/4/3</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/4/5</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/4/6</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/4/7</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
</tbody>
</table>

SPA Re-Inserted

Router# show facility-alarm status
System Totals Critical: 22 Major: 0 Minor: 0

<table>
<thead>
<tr>
<th>Source</th>
<th>Time</th>
<th>Severity</th>
<th>Description [Index]</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet0/0/0</td>
<td>May 18 2016 14:53:02</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [35]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/1</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/2</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/6</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/7</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/2/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/2/2</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link Down [1]</td>
</tr>
</tbody>
</table>
To view critical alarms specifically, use the show facility-alarm status critical command:

```
Router# show facility-alarm status critical
System Totals Critical: 22 Major: 0 Minor: 0

<table>
<thead>
<tr>
<th>Source</th>
<th>Time</th>
<th>Severity</th>
<th>Description [Index]</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet0/0/0</td>
<td>May 18 2016 14:53:02</td>
<td>CRITICAL</td>
<td>Physical Port Link Down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>GigabitEthernet0/0/1</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/2</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/3</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/5</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/7</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/2/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/2/2</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/2/3</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/2/5</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>GigabitEthernet0/2/6</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/1</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/2</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>GigabitEthernet0/4/3</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/4</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/5</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/6</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/7</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/8</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/9</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/10</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/11</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/12</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
</tbody>
</table>
```

Cisco ASR 900 Router Series Configuration Guide, Cisco IOS XE Release 3S
To view the operational state of the major hardware components on the router, use the show platform diag command. This example shows the Power supply P0 has failed:

Router# show platform diag
Chassis type: ASR903
Slot: 1, A900-RSP2A-128
  Running state : ok
  Internal state : online
  Internal operational state : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time : 00:03:41 (00:56:24 ago)
  CPLD version : 15092360
  Firmware version : 15.4(3r)S2
  Sub-slot: 0/0, A900-IMA2Z
    Operational status : ok
    Internal state : inserted
    Physical insert detect time : 00:04:46 (00:55:19 ago)
    Logical insert detect time : 00:04:46 (00:55:19 ago)
  Sub-slot: 0/1, A900-IMA8T
    Operational status : ok
    Internal state : inserted
    Physical insert detect time : 00:04:46 (00:55:19 ago)
    Logical insert detect time : 00:04:46 (00:55:19 ago)
  Sub-slot: 0/2, A900-IMA8S
    Operational status : ok
    Internal state : inserted
    Physical insert detect time : 00:04:46 (00:55:19 ago)
    Logical insert detect time : 00:04:46 (00:55:19 ago)
  Sub-slot: 0/3, A900-IMA4OS
    Operational status : ok
    Internal state : inserted
    Physical insert detect time : 00:04:46 (00:55:18 ago)
    Logical insert detect time : 00:04:46 (00:55:18 ago)
  Sub-slot: 0/4, A900-IMA8S1Z
    Operational status : ok
    Internal state : inserted
    Physical insert detect time : 00:04:46 (00:55:18 ago)
    Logical insert detect time : 00:04:46 (00:55:18 ago)
  Sub-slot: 0/5, A900-IMASER14A/S
    Operational status : ok
    Internal state : inserted
    Physical insert detect time : 00:04:46 (00:55:18 ago)
    Logical insert detect time : 00:04:46 (00:55:18 ago)
Slot: R0, A900-RSP2A-128
  Running state : ok, standby
  Internal state : online
  Internal operational state : ok
  Physical insert detect time : 00:24:37 (00:35:28 ago)
  Software declared up time : 00:31:28 (00:28:36 ago)
  CPLD version : 15092360
  Firmware version : 15.4(3r)S2
Slot: R1, A900-RSP2A-128
  Running state : ok, active
  Internal state : online
  Internal operational state : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time : 00:02:33 (00:57:31 ago)
Reviewing and Analyzing Alarm Messages

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

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

Configuring External Alarm Trigger

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

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

Onsite Network Administrator Responds to Audible or Visual Alarms

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

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

Clearing Audible and Visual Alarms

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

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

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

How to Configure External Alarms

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `alarm-contact contact-number description string`
4. `alarm-contact {contact-number | all {severity {critical | major | minor} | trigger {closed | open}}}`
5. `exit`
6. `show facility-alarm status`

**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>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

*Note* The `clear facility-alarm` command is not supported. The `clear facility-alarm` command does not clear an alarm LED on the RP faceplate or turn off the DC light bulb.
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>alarm-contact contact-number description string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)#alarm-contact 2 description door sensor</td>
</tr>
</tbody>
</table>

(Optional) Configures a description for the alarm contact number.
- The contact-number can be from 1 to 4.
- The description string can be up to 80 alphanumeric characters in length and is included in any generated system messages.

### Step 4

| alarm-contact {contact-number | all {severity {critical | major | minor} | trigger {closed | open}} |
|-----------------|--------------------------|
| Example: | Router(config)#alarm-contact 2 severity major |

Configures the trigger and severity for an alarm contact number or for all contact numbers.
- Enter a contact number (1 to 4) or specify that you are configuring all alarms.
- For severity, enter critical, major, or minor. If you do not configure a severity, the default is minor.
- For trigger, enter open or closed. If you do not configure a trigger, the alarm is triggered when the circuit is closed.

### Step 5

<table>
<thead>
<tr>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
</tr>
</tbody>
</table>

Exits the configuration mode.

### Step 6

<table>
<thead>
<tr>
<th>show facility-alarm status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
</tr>
</tbody>
</table>

Displays configured alarms status.

### Example

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

<table>
<thead>
<tr>
<th>Source</th>
<th>Time</th>
<th>Severity</th>
<th>Description [Index]</th>
</tr>
</thead>
<tbody>
<tr>
<td>subslot 0/0</td>
<td>Sep 21 2016 15:19:55</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR [0]</td>
</tr>
<tr>
<td>Alarm (0)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subslot 0/1</td>
<td>Sep 21 2016 15:19:12</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR [0]</td>
</tr>
<tr>
<td>Alarm (0)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subslot 0/2</td>
<td>Sep 21 2016 15:16:59</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR [0]</td>
</tr>
<tr>
<td>Alarm (0)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subslot 0/3</td>
<td>Sep 21 2016 15:18:10</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR [0]</td>
</tr>
<tr>
<td>Alarm (0)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subslot 0/5</td>
<td>Sep 21 2016 15:16:11</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR [0]</td>
</tr>
</tbody>
</table>
The external alarm trigger and syslog support configuration is supported from Cisco IOS XE Release 3.13.0S.

**Alarm Filtering Support**

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

**Information About Alarm Filtering Support**

**Overview of Alarm Filtering Support**

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

**CISCO-ENTITY-ALARM-MIB**

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

**ceAlarmGroup**

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

Following are the objects in ceAlarmGroup:

- ceAlarmCriticalCount
- ceAlarmMajorCount
ceAlarmFilterProfileTable

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

ceAlarmFilterProfile

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

ceAlarmHistTable:

This table contains the history of ceAlarmAsserted and ceAlarmCleared traps generated by the agent. Each entry to the table will have physical index from entPhysicalTable and the severity of the alarm.

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

ceAlarmDescrTable:

This table contains a description for each alarm type defined by each vendor type employed by the system. This table has the list of possible severity levels and the description for the physical entity, Object “ceAlarmDescrSeverity” indicates the severity of an alarm (1 to 4 as above).

ceAlarmTable:

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

Prerequisites for Alarm Filtering Support

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

Restrictions for Alarm Filtering Support

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

Configuring Alarm Filtering for Syslog Messages

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

```
enable
configure terminal
logging alarm 2
show facility-alarm status
```

Configuring Alarm Filtering for SNMP Notifications

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

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

Configuration Examples for Alarm Filtering Support

Configuring Alarm Filtering for Syslog Messages: Example

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

```
Router# enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# snmp-server enable traps alarms 2
Router(config)# exit
Router# show facility-alarm status
```

System Totals Critical: 2 Major: 1 Minor: 0

<table>
<thead>
<tr>
<th>Source</th>
<th>Time</th>
<th>Severity</th>
<th>Description [Index]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply Bay 0</td>
<td>Jun 07 2016 13:36:49</td>
<td>CRITICAL</td>
<td>Power Supply/FAN Module</td>
</tr>
<tr>
<td>xcvr container 0/5/0</td>
<td>Jun 07 2016 13:37:43</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/5/1</td>
<td>Jun 07 2016 13:37:43</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/5/2</td>
<td>Jun 07 2016 13:37:43</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/5/3</td>
<td>Jun 07 2016 13:37:43</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/5/4</td>
<td>Jun 07 2016 13:37:43</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/5/5</td>
<td>Jun 07 2016 13:37:43</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/5/6</td>
<td>Jun 07 2016 13:37:43</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
</tbody>
</table>

Configuring Alarm Filtering for SNMP Notifications: Example

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

```
```
Configuring Alarm Filtering for SNMP Notifications: Example

xcvr container 0/5/7       Jun 07 2016 13:37:43       INFO       Transceiver Missing [0]
CHAPTER 20

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) - The encapsulation type is OTU1e and OTU2e.
- 2-port 40 Gigabit Ethernet QSFP Interface Module (2x40GE) (A900-IMA2F) - The encapsulation type is OTU3.
- 1-port 100 Gigabit Ethernet Interface Module (1X100GE) (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, into the corresponding OTU1e or OTU2e, OTU3 containers, respectively. This enables the ports of the interface modules to work in layer 1 optical mode in conformance with standard G.709.
OTN Frame

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

- Advantages of OTN, on page 347
- ODU and OTU, on page 347
- Deriving OTU1e and OTU2e Rates, on page 347
- OTU1e and OTU 2e Support on 8x10GE Interface Module, on page 348
- OTU3 Support in 2x40GE Interface Module, on page 349
- OTU4 Support on 1-port 100 Gigabit Ethernet Interface Module (1X100GE), on page 349
- Supported Transceivers, on page 349
- OTN Specific Functions, on page 349
- Standard MIBS, on page 350
- Restrictions for OTN, on page 350
- DWDM Provisioning, on page 351
- Configuring Transport Mode in 8x10GE and 2x40GE Interface Modules, on page 351
- Configuring Transport Mode in 1X100GE Interface Module, on page 354
- OTN Alarms, on page 356
- OTN Threshold, on page 359
- Configuring OTU Alerts, on page 361
- Configuring ODU Alerts, on page 361
- Configuring ODU Alerts, on page 361
- Loopback, on page 363
- Configuring Loopback, on page 363
- Forward Error Connection, on page 364
- SNMP Support, on page 367
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:
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:

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

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, are used for 8x10GE, 2x40GE 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.
• FECMISMATCH alarm is not supported.
• Enhanced FEC is not supported.
• Alarm and error counters are visible when the controller is in shutdown state.

**DWDM Provisioning**

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

**Prerequisites for DWDM Provisioning**

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

**Configuring DWDM Provisioning**

Use the following commands to configure DWDM provisioning:

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

**Configuring Transport Mode in 8x10GE and 2x40GE Interface Modules**

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

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

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

**Note**

LAN transport mode is the default mode.

To configure the transport administration state on a DWDM port, use the `admin-state` command in DWDM configuration mode. To return the administration state from a DWDM port to the default, use the `no` form of this command.
Verification of LAN Transport Mode Configuration

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

```
Router#sh int te0/1/0
TenGigabitEthernet0/1/0 is up, line protocol is up
  MTU 1500 bytes, BW 1000000 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
    2657188335 packets input, 1700600465344 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    1076664813 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
```
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, 100000Mbps, link type is force-up, media type is CPAK-100G-SR10
output flow-control is off, input flow-control is off
Transport mode OTN OTU4 (111.80997Gb/s)
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP Multicasts)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 2 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out

#show controllers dwdm 0/8/0
G709 Information:
Controller dwdm 0/8/0, is up (no shutdown)
Transport mode OTN OTU4
Loopback mode enabled : None
TAS state is : IS
G709 status : Enabled

OTU
  LOS = 0
  AIS = 0
  TIM = 0

ODU
  AIS = 0
  OCI = 0
  BIP = 0

FEC Mode: None
Remote FEC Mode: Unknown
  FECM = 0
  EC(current second) = 0
  EC = 0
  UC = 0

Detected Alarms: NONE
asserted Alarms: NONE
Detected Alerts: NONE
asserted Alerts: NONE

Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI OTU-TIM ODU-AIS ODU-OCI
  ODU-LCK ODU-BDI ODU-PTIM ODU-TIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3 ODU-SD = 10e-6 OTU-SF = 10e-3 OTU-SD = 10e-6
TCA thresholds: SM = 10e-3 PM = 10e-3

OTU TTI Sent  String SAPI ASCII : Tx TTI Not Configured
OTU TTI Sent  String DAPI ASCII : Tx TTI Not Configured
OTU TTI Sent  String OPERATOR ASCII : Tx TTI Not Configured
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:

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

---

**Note**

Fecmismatch is not supported.

---

**Note**

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

### Verification of OTU Alarm Reports Configuration

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

```plaintext
#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
```

---

OTN Wrapper Overview
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

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

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

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 : 0000000000000000000000000000000000000000000

Syslog Generation for LOS Alarm

The following example shows the syslog generation for LOS alarm:

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

Configuring ODU Alarm Report

Use the following commands to configure ODU alarm reports:

```
enable
configure terminal
controller dwdm 0/4/1
shut
```
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
cfg-term
con 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
cfg-term
con 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 (10GBASE-R over OPU1e w/o fixed stuffing, 11.0491Gb/s)
Loopback mode enabled : None

TAS state is : UNKNWN
G709 status : Enabled

OTU

<table>
<thead>
<tr>
<th>alarms</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOS</td>
<td>0</td>
</tr>
<tr>
<td>LOF</td>
<td>0</td>
</tr>
<tr>
<td>LOM</td>
<td>0</td>
</tr>
<tr>
<td>AIS</td>
<td>0</td>
</tr>
<tr>
<td>BDI</td>
<td>0</td>
</tr>
<tr>
<td>BIP</td>
<td>0</td>
</tr>
<tr>
<td>TIM</td>
<td>0</td>
</tr>
<tr>
<td>IAE</td>
<td>0</td>
</tr>
<tr>
<td>BEI</td>
<td>0</td>
</tr>
</tbody>
</table>

ODU

<table>
<thead>
<tr>
<th>alarms</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>0</td>
</tr>
<tr>
<td>BDI</td>
<td>0</td>
</tr>
<tr>
<td>TIM</td>
<td>0</td>
</tr>
<tr>
<td>OCI</td>
<td>0</td>
</tr>
<tr>
<td>LCK</td>
<td>0</td>
</tr>
<tr>
<td>PTIM</td>
<td>0</td>
</tr>
<tr>
<td>BIP</td>
<td>0</td>
</tr>
<tr>
<td>BEI</td>
<td>0</td>
</tr>
</tbody>
</table>

FEC Mode: FEC

Remote FEC Mode: Unknown

<table>
<thead>
<tr>
<th>alarms</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FECM</td>
<td>0</td>
</tr>
<tr>
<td>EC</td>
<td>0</td>
</tr>
<tr>
<td>UC</td>
<td>0</td>
</tr>
</tbody>
</table>

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-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3 ODU-SD = 10e-6 OTU-SF = 10e-3 OTU-SD = 10e-6
TCA thresholds: SM = 10e-3 PM = 10e-3

OTU TTI Sent String SAPI ASCII : AABBCCDD
OTU TTI Sent String DAPI ASCII : AABBCCDD
OTU TTI Sent String OPERATOR ASCII : AABBCCDD
OTU TTI Expected String SAPI ASCII : AABBCCDD
OTU TTI Expected String DAPI ASCII : AABBCCDD
OTU TTI Expected String OPERATOR HEX : AABBCCDD
OTU TTI Received String HEX : 0052414D45534800000000000000000241D455348000

ODU TTI Sent String SAPI ASCII : AABBCCDD
ODU TTI Sent String DAPI ASCII : AABBCCDD
ODU TTI Sent String OPERATOR HEX : 11223344
ODU TTI Expected String SAPI ASCII : AABBCCDD
ODU TTI Expected String DAPI ASCII : AABBCCDD
ODU TTI Expected String OPERATOR HEX : 11223344
ODU TTI Received String HEX : 0052414D45534800000000000000000241D455348000

Configuring OTU Alerts

To configure OTU alerts:

```
enable
custom terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
g709 otu threshold sd-ber
no shutdown
end
```

Configuring ODU Alerts

To configure ODU alerts:

```
enable
custom terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
g709 otu threshold pm-tca
no shutdown
end
```

Verifying Alerts Configuration

Use the show controllers command to verify the alerts configuration:

```
#show controllers dwdm 0/4/1
G709 Information:
Controller dwdm 0/4/1, is down (shutdown)
```
Transport mode OTN OTU3
Loopback mode enabled: Line

TAS state is: IS
G709 status: Enabled

OTU
LOS = 5  LOF = 1  LOM = 0
AIS = 0  BDI = 0  BIP = 149549
TIM = 0  IAE = 0  BEI = 74685

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

FEC Mode: FEC
Remote FEC Mode: Unknown
FECM = 0
EC (current second) = 0
EC = 856
UC = 23165

Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE

Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-5
TCA thresholds: SM = 10e-3  PM = 10e-4

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

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

- Internal Loopback - All packets are looped back internally within the router before reaching an external cable. It tests the internal Rx to Tx path and stops the traffic to egress out from the Physical port.
- Line Loopback - Incoming network packets are looped back through the external cable.

Configuring Loopback

To configure loopback:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
loopback line
no shutdown
end
```

Verifying Loopback Configuration

Use the `show controllers` command to verify the loopback configuration:

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

Controller dwdm 0/4/1, is up (no shutdown)
Transport mode OTN OTU3
Loopback mode enabled : Line

TAS state is : IS
G709 status : Enabled

OTU
  LOS = 5  LOF = 1  LOM = 0
  AIS = 0  BDI = 0  BIP = 149549
  TIM = 0  IAE = 0  BEI = 74685

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

FEC Mode: FEC
Remote FEC Mode: Unknown
  FECM = 0
  EC(current second) = 0
  EC = 856
  UC = 23165

Detected Alarms: NONE
```
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:

```plaintext
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 fec standard
no shutdown
end
```

Verifying FEC Configuration

Use the `show controllers` command to verify FEC configuration:

```
G709 Information:
Controller dwdm 0/4/1, is up (no shutdown)
Transport mode OTN OTU3
Loopback mode enabled : Line
TAS state is : IS
G709 status : Enabled

OTU
  LOS = 5  LOF = 1  LOM = 0
  AIS = 0  BDI = 0  BIP = 149549
  TIM = 0  IAE = 0  BEI = 74685

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

FEC Mode: FEC
Remote FEC Mode: Unknown <- This is a limitation by which we do not show the remote FEC mode
   FECM = 0
   EC(current second) = 0
   EC = 856  <- This is the counter for Error corrected bits .
   UC = 23165  <- this is the counter for Uncorrected alarms .
```

Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE

Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-5
TCA thresholds: SM = 10e-3  PM = 10e-4

OTU TTI Sent String SAPI ASCII : Tx TTI Not Configured
OTU TTI Sent String DAPI ASCII : Tx TTI Not Configured
OTU TTI Sent String OPERATOR ASCII : Tx TTI Not Configured
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:

```bash
enable
configure terminal
controller dwm 0/1/1
shutdown
g709 tti-processing enable
no shutdown
derm
```

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:

```bash
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:

```snmp
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 ASCII : AABBCCDD
OTU TTI Expected String OPERATOR HEX : AABBCCDD
OTU TTI Received String HEX : 0052414D45534800000000000000000052414D4553480000
0000000000000041414242434344000000000000000000000000
000000000000000000000000

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 17: 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 34: 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 background block errors ratio recorded in the OTN path during the PM time interval.</td>
</tr>
<tr>
<td>BBER-SM</td>
<td>Section Monitoring Background Block Errors Ratio (BBER-SM) indicates the background block errors ratio recorded in the OTN section during the PM time interval.</td>
</tr>
<tr>
<td>ES-PM</td>
<td>Path Monitoring Errored Seconds (ES-PM) indicates the errored seconds 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 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 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 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 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 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 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 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 severely errored seconds ratio recorded in the OTN path during the PM time interval.</td>
</tr>
</tbody>
</table>
The following table shows the details of each type of PM parameter for FEC:

<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>

**OTUk Section Monitoring**

Section Monitoring (SM) overhead for OTUk is terminated as follows:

- TTI
- BIP
- BEI
- BDI
- IAE
- BIAE

BIP and BEI counters are block error counters (block size equal to OTUk frame size). The counters can be read periodically by a PM thread to derive one second performance counts. They are sufficiently wide for software to identify a wrap-around with up to 1.5 sec between successive readings.

The following OTUk level defects are detected:

- dAIS
- dTIM
- dBDi
• dIAE
• dBIAE

Status of the defects is available through CPU readable registers, and a change of status of dLOF, dLOM, and dAIS will generate an interruption.

**ODUk Path Monitoring**

Path Monitoring (PM) overhead for higher order ODUk and lower order ODUk is processed as follows:

• TTI
• BIP
• BEI
• BDI
• STAT including ODU LCK/OCI/AIS

The following ODUk defects are detected:

• dTIM
• dLCK and dAIS (from STAT field)
• 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:

```
enable
cfg-term
ct-ctrl dwdm 0/1/0
pm 15-min fec report ec-bits enable
pm 15-min fec report uc-words enable
end
```

To set TCA report status on FEC layer in 24-hour interval:

```
enable
cfg-term
ct-ctrl dwdm 0/1/0
pm 24-hr fec report ec-bits enable
pm 24-hr fec report uc-words enable
end
```

To set threshold on FEC layer in 15-minute interval:

```
enable
cfg-term
ct-ctrl 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:

```bash
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:

```bash
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:

```bash
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:

```bash
enable
configure terminal
controller dwdm 0/1/0
pm 15-min otn threshold es-pm-ne enable
end
```

To set OTN threshold in 24-hour interval:

```bash
enable
configure terminal
controller dwdm 0/1/0
pm 24-hr otn threshold es-pm-ne enable
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
SES-SM-NE : 0.00000 Threshold : 0.02300 TCA(enable) : NO
UAS-SM-NE : 0 Threshold : 0 TCA(enable) : NO
BBER-SM-NE : 0.00000 Threshold : 0.02300 TCA(enable) : NO
FC-SM-NE : 0 Threshold : 0 TCA(enable) : NO
ES-PM-NE : 0 Threshold : 200 TCA(enable) : YES
ESR-PM-NE : 0.00000 Threshold : 1.00000 TCA(enable) : NO
SES-PM-NE : 0 Threshold : 0 TCA(enable) : NO
SES-PM-NE : 0.00000 Threshold : 0.02300 TCA(enable) : NO
UAS-PM-NE : 0 Threshold : 0 TCA(enable) : NO
BBER-PM-NE : 0.00000 Threshold : 0.02300 TCA(enable) : NO
FC-PM-NE : 0 Threshold : 0 TCA(enable) : NO
```

```
OTN Far-End Valid : YES
ES-SM-FE : 0 Threshold : 0 TCA(enable) : NO
ESR-SM-FE : 0.00000 Threshold : 1.00000 TCA(enable) : NO
SES-SM-FE : 0 Threshold : 0 TCA(enable) : NO
SES-SM-FE : 0.00000 Threshold : 0.02300 TCA(enable) : NO
UAS-SM-FE : 0 Threshold : 0 TCA(enable) : NO
BBER-SM-FE : 0.00000 Threshold : 0.02300 TCA(enable) : NO
FC-SM-FE : 0 Threshold : 0 TCA(enable) : NO
ES-PM-FE : 0 Threshold : 0 TCA(enable) : NO
ESR-PM-FE : 0.00000 Threshold : 1.00000 TCA(enable) : NO
SES-PM-FE : 0 Threshold : 0 TCA(enable) : NO
SES-PM-FE : 0.00000 Threshold : 0.02300 TCA(enable) : NO
UAS-PM-FE : 0 Threshold : 0 TCA(enable) : NO
BBER-PM-FE : 0.00000 Threshold : 0.02300 TCA(enable) : NO
FC-PM-FE : 0 Threshold : 0 TCA(enable) : NO
```

Router#show controllers dwdm 0/1/0 pm interval 15-min otn 1

```
g709 OTN in interval 1 [9:00:00 - 9:15:00 Thu Jun 9 2016]
```

OTN current bucket type: VALID
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 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

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
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

<table>
<thead>
<tr>
<th>OTN Near-End Valid</th>
<th>OTN Far-End Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES-SM-NE</td>
<td>7</td>
<td>ESR-SM-NE</td>
<td>0.00000</td>
</tr>
<tr>
<td>SES-SM-NE</td>
<td>7</td>
<td>SESR-SM-NE</td>
<td>0.00000</td>
</tr>
<tr>
<td>SSSR-SM-NE</td>
<td>0.00000</td>
<td>SES-SM-FE</td>
<td>0</td>
</tr>
<tr>
<td>UAS-SM-NE</td>
<td>41</td>
<td>BBER-SM-NE</td>
<td>0.00000</td>
</tr>
<tr>
<td>BBE-SM-NE</td>
<td>0</td>
<td>BBER-PM-NE</td>
<td>0.00000</td>
</tr>
<tr>
<td>FC-SM-NE</td>
<td>3</td>
<td>FC-SM-FE</td>
<td>0</td>
</tr>
<tr>
<td>ES-PM-NE</td>
<td>2</td>
<td>ESR-PM-NE</td>
<td>0.00000</td>
</tr>
<tr>
<td>SES-PM-NE</td>
<td>0</td>
<td>SESR-PM-NE</td>
<td>0.00000</td>
</tr>
<tr>
<td>UAS-PM-NE</td>
<td>0</td>
<td>BBE-PM-NE</td>
<td>3</td>
</tr>
<tr>
<td>BBER-PM-NE</td>
<td>0.00000</td>
<td>BBER-PM-FE</td>
<td>1</td>
</tr>
<tr>
<td>FC-PM-NE</td>
<td>0</td>
<td>FC-PM-FE</td>
<td>0</td>
</tr>
</tbody>
</table>

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. Check for TTI Mismatch. Verify the major alarms. Verify the FEC mode. 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>
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 Cisco ASR 900 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 also provided with the devices in the distribution layer and that support both 1G and 10G traffic. Thus, all the eight ports can now work in 1G mode as well as 10G mode.

The configuration of 1G Traffic on 8X10GE IM provides cost-effective solution during migration from 1G mode to 10G mode as a single device can support both the modes. The feature is supported on Cisco ASR 900 RSP3 module.

By default, the 8X10GE IM comes up in the 10G mode after reboot.

Note

• Restrictions for 1G Mode Support on 8-port 10 Gigabit Ethernet Interface Module, on page 379
• Configuring 1G Mode, on page 380
• Configuring 10G Mode from 1G Mode, on page 381
• Associated Commands, on page 382

Restrictions for 1G Mode Support on 8-port 10 Gigabit Ethernet 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.
• 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, te0/4/0, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full Duplex, 1000Mbps, link type is auto, media type is SX
output flow-control is off, input flow-control is off
Transport mode LAN (1Gb/s)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:08:24, output 00:08:24, output hang never
Last clearing of "show interface" counters 00:07:59
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
```

To verify the slots configured in 1G mode, use the `show running-config | i ether-mode` command in privileged EXEC mode:

```
Router#show running-config | i ether-mode
hw-module subslot 0/3 ether-mode 1g
hw-module subslot 0/4 ether-mode 1g
hw-module subslot 0/11 ether-mode 1g
```
To verify the bandwidth and port speed, use the `show platform hardware pp active interface all` in privileged EXEC mode:

```
Router#show platform hardware pp active interface all
    Interface manager platform keys
    -----------------------------
    Name: TenGigabitEthernet0/4/7, Asic: 0, hwidx: 9
    lpn: 0, ppn: 9, gid: 9, mac: c8f9.f98d.202b
    InLportId: 0, ELportId: 0, dpidx: 31, l3ID: 25
    port_flags: 0, **port_speed: 1000 Mbps**, efp_count: 0, destIndex: 9, intType: 1
    etherchnl: 0, efp: 0, bdi: 0, l2PhysIf: 0, l3PhysIf: 1, l3TDM: 0, loopBack: 0
    tunnel: 0, tunneltlp: 0, icmp_flags: 0, icmp6_flags: 0
    bandwidth: **1000000**, fcid: 0, cid: 0, mpls_tbid: 0, protocols: 4
    v4_netsmask: 8, v4_tableid: 8, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
    bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
    vrfid: 8, enctype: 0, admin_state: 1, admin_state_oir: 0

    Name: TenGigabitEthernet0/4/6, Asic: 0, hwidx: 10
    lpn: 0, ppn: 10, gid: 10, mac: c8f9.f98d.202a
    InLportId: 0, ELportId: 0, dpidx: 30, l3ID: 24
    port_flags: 0, **port_speed: 1000 Mbps**, efp_count: 0, destIndex: 10, intType: 1
    etherchnl: 0, efp: 0, bdi: 0, l2PhysIf: 0, l3PhysIf: 1, l3TDM: 0, loopBack: 0
    tunnel: 0, tunneltlp: 0, icmp_flags: 0, icmp6_flags: 0
    bandwidth: **1000000**, fcid: 0, cid: 0, mpls_tbid: 0, protocols: 4
    v4_netsmask: 8, v4_tableid: 6, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
    bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
    vrfid: 6, enctype: 0, admin_state: 1, admin_state_oir: 0
```

## Configuring 10G Mode from 1G Mode

### Defauling 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, pnn: 9, gid: 9, mac: c8f9.f98d.202b
  InPortId: 0, EPortId: 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, L2_PHYIf: 0, L3_PHYIf: 1, L3TDM: 0, loopBack: 0
  tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
  bandwidth: 100000000, 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, pnn: 10, gid: 10, mac: c8f9.f98d.202a
  InPortId: 0, EPortId: 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, L2_PHYIf: 0, L3_PHYIf: 1, L3TDM: 0, loopBack: 0
  tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
  bandwidth: 100000000, 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>
CHAPTER 22

Configuring Access Circuit Redundancy

This chapter provides information about the Access Circuit Redundancy (ACR) feature on the Cisco ASR 903 Router.

- New and Changed Information, on page 385
- Prerequisites for Configuring ACR, on page 385
- Restrictions for Configuring ACR, on page 386
- Information About ACR, on page 387
- How to Configure ACR, on page 387
- Troubleshooting the ACR configuration, on page 405
- Additional References, on page 405

New and Changed Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>ASR 903 RSP1 Module</th>
<th>ASR 903 RSP2 Module</th>
<th>ASR 902 Router</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEM ACR</td>
<td>Cisco IOS XE Release 3.10S</td>
<td>Cisco IOS Release 3.14S</td>
<td>Cisco IOS XE Release 3.12S</td>
<td></td>
</tr>
<tr>
<td>ATM ACR</td>
<td>Cisco IOS XE Release 3.12</td>
<td>NA</td>
<td>Cisco IOS XE Release 3.12S</td>
<td></td>
</tr>
</tbody>
</table>

Prerequisites for Configuring ACR

- When configured as a part of the ACR group, the Working and Protect interfaces should be of same framing type.
- When Circuit Emulation (CEM) interfaces are created, they are not ACR enabled. You must configure CEM only under the virtual Synchronous Optical Networking (SONET) controller to enable ACR.
Restrictions for Configuring ACR

- Physical or soft IM OIR causes the APS switchover time to be higher (500 to 600 ms). Shut or no shut of the port and removal of the active working or protect also cause the APS switchover time to be high. To overcome these issues, force the APS switchover.

- On the RSP3 module, it takes a long time (more than half an hour) to copy scale configuration (8064 VT CEP) from bootflash to running configuration. To overcome this issue, you can copy the configuration one by one from the CLI.

Restrictions for CEM ACR

- ACR configuration is only supported with a Single Router Automatic Protection Switching (SR-APS) configuration. For more information about APS, see Time Division Multiplexing Guide

- Maximum of 12 ACR groups are supported on the router. A single IM supports only 2 ACR groups.

- Only one virtual controller is available for every ACR group.

- An ACR group supports only two member interfaces; Working interface and Protect interface.

- CEM-ACR interfaces cannot simultaneously support both Circuit Emulation Services over Packet (CESoP) and Structure-Agnostic Time Division Multiplexing over Packet (SAToP).

- Quality of Service (QoS) is not supported on a CEM-ACR interface except for default experimental bits (EXP) marking for Multiprotocol Label Switching (MPLS) pseudowires.

- CEM ACR is not supported on the RSP3 module in Cisco IOS XE Release 3.16.1S.

Restrictions for ATM ACR

- ATM ACR is not supported on the RSP3 module in Cisco IOS XE Release 3.16.1S.

- ACR configuration is only supported with a Single Router Automatic Protection Switching (SR-APS) configuration. For more information about APS, see.

- Maximum of 12 ACR groups are supported on the router. A single IM supports only 2 ACR groups.

- Only one virtual controller is available for every ACR group.

- An ACR group supports only two member interfaces; Working interface and Protect interface.

- Quality of Service (QoS) is not supported on a ATM-ACR interface except for default experimental bits (EXP) marking for Multiprotocol Label Switching (MPLS) pseudowires.

- For successful ATM ACR switchover, configuration of VCs must be the same for both working and protect interfaces. The switchover time is less than 200 ms.

- ATM-ACR PVP mode is not supported in Cisco IOS XE Release 3.12S.

- A delay of 8 seconds per PVC is required between every ACR switchover. For N number of PVCs, N*8 seconds of delay is required between every ACR switchover. Following are the trigger for ACR switchover:
  - Reloading the IM with ACR port configuration
  - Executing shutdown command followed by a no shutdown command
  - Flapping of active port link
  - Removing or inserting a cable of active port.
• The maximum number of ACR-ATM interfaces supported in SONET mode is 84.
• The maximum number of ACR-ATM interfaces supported in SDH mode is 63.
• Configuring ATM followed by ACR-ATM configuration results in Standby RSP crashes. To migrate the ATM configuration to ACR-ATM or vice-versa, perform the following:
  • Remove the ATM configuration
  • Save the configuration and perform a reload
  • Upload a new image on the router
  • Configure the ACR-ATM feature

• Unidirectional traffic may drop after multiple ACR switch covers and when SSO is performed.
• Maintenance tasks such as performing shutdown followed by a no shutdown at the virtual controller or interface are not allowed.

Information About ACR

CEM ACR

ACR enables local switching for CEM interfaces by creating a virtual CEM-ACR interface. All configuration changes made on the virtual CEM-ACR interface are applied automatically on both the working and protect interfaces. Switching from working to protect or protect to working interface occurs within 250 milliseconds at different scaled levels with line rate traffic.

The virtual CEM-ACR interface provides the simplicity of a single point of configuration and the flexibility of not running a backup pseudowire for the protect interface in a failure.

ATM ACR

ATM ACR interfaces are created at the ACR controller and the PVC are created at the virtual ACR interface. For each virtual interface one working and one protect interface (physical) exist. At any instance, only one interface is active.

The virtual interface state represents the active interface state. PVC’s are created in the virtual interfaces.

How to Configure ACR

Configuring ACR (SONET Framing)

SUMMARY STEPS

1. enable
2. configure terminal
3. controller sonet slot/subslot/port
4. framing sonet
5. clock source {internal | line}
6. aps group acr acr-no
### Configuring Access Circuit Redundancy

#### 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>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><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> controller sonet slot/subslot/port</td>
<td>Selects the work controller to configure and enters controller configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# controller sonet 0/1/0</td>
<td>• <code>slot/subslot/port</code> — Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> framing sonet</td>
<td>Configures the framing mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (config-controller)# framing sonet</td>
<td>• <code>sonet</code> — Enables SONET framing.</td>
</tr>
<tr>
<td><strong>Step 5</strong> clock source {internal</td>
<td>line}</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (config-controller)# clock source internal</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <code>internal</code> — Specifies that the internal clock source is used.</td>
</tr>
<tr>
<td></td>
<td>• <code>line</code> — Specifies that the network clock source is used. This is the default for T1 and E1.</td>
</tr>
<tr>
<td><strong>Step 6</strong> aps group acr acr-no</td>
<td>Configures the APS group for the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-controller)# aps group acr 1</td>
<td>• <code>acr</code> — Configures the ACR group on top of APS.</td>
</tr>
<tr>
<td></td>
<td>• <code>acr-no</code> — A group number that is valid between 1 and 96. Any group number exceeding this range is not supported.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 7</th>
<th><code>aps working circuit-number</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router (config-controller)# aps working 1</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th><code>exit</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router (config-controller)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th><code>controller sonet slot/subslot/port</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router (config)# controller sonet 0/2/0</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th><code>aps group acr acr-no</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-controller)# aps group acr 1</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th><code>aps protect circuit-number ip-address</code></th>
</tr>
</thead>
</table>

### Purpose

- For Cisco ASR 900 RSP1 Module, the valid group number is between 1 and 96.
- For Cisco ASR 900 RSP2 Module, the valid group number is between 1 and 192.

Note

The APS group can be either active or inactive:

- Active—The interface that is currently sending and receiving data.
- Inactive—The interface that is currently standing by to take over when the active fails.

- `circuit-number`—Identification number for this particular channel in the APS pair. Since the interface only supports 1+1 redundancy, the only valid and the default value for working interface is 1.

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

- `acr-no`—A group number that is valid between 1 and 96. Any group number exceeding this range is not supported.

- `for Cisco ASR 900 RSP1 Module, the valid group number is between 1 and 96.
- For Cisco ASR 900 RSP2 Module, the valid group number is between 1 and 192.

Note
### Configuring ACR (SDH Framing)

**SUMMARY STEPS**

1. enable
2. configure terminal
3. controller sonet slot/subslot/port
4. framing sdh
5. clock source {internal | line}
6. aps group acr acr-no
7. aps working circuit-number
8. exit
9. controller sonet slot/subslot/port

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>```</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# aps protect 1 4.1.1.1</td>
<td>- <em>circuit-number</em> — Identification number for this particular channel in the APS pair. Because only 1+1 redundancy is supported, the only valid value is 1, and the Protect interface defaults to 1.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td>aps revert minutes</td>
<td>(Optional) Configures the ACR interface as revert.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>```</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# aps revert 2</td>
<td>- <em>minutes</em> — Specifies the time, in minutes, after which the revert process begins.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits controller configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>```</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

The following is a sample configuration of ACR using SONET framing:

```bash
Router# Configure terminal
Router(config)# Controller sonet 0/1/0
Router(config-controller)# aps group acr 1
Router(config-controller)# aps working 1
Router(config-controller)# exit
Router(config)# controller sonet 0/2/0
Router(config-controller)# aps group acr 1
Router(config-controller)# aps protect 1 4.1.1.1
Router(config-controller)# do show ip interface brief | incl Loop
Loopback0  4.1.1.1   YES NVRAM  up     up
Router(config-controller)#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.   | controller sonet slot/subslot/port | Selects the work controller to configure and enters controller configuration mode.  
      | Example:          | • slot/subslot/port — Specifies the location of the interface. |
|      | Router (config)# controller sonet 0/0/2 |         |
| 4.   | framing sdh       | Configures the framing mode.  
      | Example:          | • sdh—Enables SDH framing for STM rates. |
|      | Router (config-controller)# framing sdh |         |
| 5.   | clock source {internal | line} | Sets the clock source.  
      | Example:          | 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. |
|      | Router (config-controller)# clock source internal |         |
| 6.   | aps group acr acr-no | Configures the APS group for the controller.  
      | Example:          | • acr—Configures the ACR group on top of APS.  
      |                  | • acr-no—A group number that is valid between 1 and 96. Any group number exceeding this range is not supported. |
|      | Router (config-controller)# aps group acr 1 |         |
Configuring ACR (SDH Framing)

### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Note**          | • For Cisco ASR 900 RSP1 Module, the valid group number is between 1 and 96.  
                  | • For Cisco ASR 900 RSP2 Module, the valid group number is between 1 and 192.  

The APS group can be either active or inactive:

• Active—The interface that is currently sending and receiving data.

• Inactive—The interface that is currently standing by to take over when the active fails.

### Step 7

**aps working circuit-number**

Example:

Router (config-controller)# **aps working 1**

### Step 8

**exit**

Example:

Router (config-controller)# **exit**

### Step 9

**controller sonet slot/subslot/port**

Example:

Router (config)# **controller sonet 0/2/0**

### Step 10

**aps group acr acr-no**

Example:

Router(config-controller)# **aps group acr 1**

### Step 11

**aps protect circuit-number ip-address**

Identifies the interface as the Protect interface.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
| Router(config-controller)# **aps protect 1 4.1.1.1** | • *circuit-number* — Identification number for this particular channel in the APS pair. Because only 1+1 redundancy is supported, the only valid value is 1, and the Protect interface defaults to 1.  
• *ip-address* — IP address for the loopback interface. The Protect interface uses this IP address to communicate with the Working interface. |
| **Step 12**       |         |
| **aps revert minutes** | (Optional) Configures the ACR interface as revert.  
• minutes — Specifies the time, in minutes, after which the revert process begins. |
| Example:          |         |
| Router(config-controller)# **aps revert 2** | Note Use the **aps revert** command only under the protect member of the ACR group. |
| **Step 13**       |         |
| **exit**          |         |
| Example:          |         |
| Router (config-controller)# **exit** | Exits controller configuration mode. |

**What to do next**

The following is a sample configuration of ACR interface using SDH framing:

```bash
Router# configure terminal
Router(config)# controller sonet 0/0/2
Router(config-controller)# framing sdh
Router(config-controller)# clock source internal
Router(config-controller)# aps group acr 10
Router(config-controller)# aps working 1
Router(config-controller)# exit
Router# configure terminal
Router(config)# controller sonet 0/0/3
Router(config-controller)# framing sdh
Router(config-controller)# clock source internal
Router(config-controller)# aps group acr 10
Router(config-controller)# aps protect 1 22.22.22.22
Router(config-controller)# exit
```

**Configuring CEM (SONET Framing)**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. **controller sonet-acr acr_no**
4. **sts-1 number**
5. **vtg vtg-number t1 t1-line-number cem-group group number unframed**
6. OR,  
7. exit
## 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>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> controller sonet-acr acr_no</td>
<td>Selects the controller to configure.</td>
</tr>
<tr>
<td>Example:</td>
<td>• acr_no — Specifies the controller unit number.</td>
</tr>
<tr>
<td>Router (config)# controller sonet-acr 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sts-1 number</td>
<td>Specifies the STS identifier.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router (config-controller)# sts-1 1</td>
</tr>
<tr>
<td><strong>Step 5</strong> vtg vtg-number t1 t1-line-number cem-group group number unframed</td>
<td>Creates a single Structure-Agnostic TDM over Packet (SAToP) CEM group.</td>
</tr>
<tr>
<td>Example:</td>
<td>• vtg — Specifies the vtg number from 1-7.</td>
</tr>
<tr>
<td></td>
<td>• t1-line-number — Identifies the T1 line number from 1 to 4.</td>
</tr>
<tr>
<td></td>
<td>• cem-group — Creates a circuit emulation channel from one or more timeslots of a T1 or E1 line.</td>
</tr>
<tr>
<td></td>
<td>• group-number — Identifies the channel number to be used for this channel from 0-215.</td>
</tr>
<tr>
<td></td>
<td>• unframed — Specifies that a single CEM channel is being created including all timeslots and the framing structure of the line.</td>
</tr>
<tr>
<td>Router (config-ctrlr-sts1)# vtg 1 t1 1 cem-group 1 unframed</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> OR,</td>
<td>Creates a Circuit Emulation Services over Packet Switched Network (CESoPSN) CEM group.</td>
</tr>
<tr>
<td>Example:</td>
<td>• timeslots — Specifies the timeslots to be included in the CEM channel.</td>
</tr>
<tr>
<td>vtg vtg-number t1 t1-line-number cem-group group number timeslots timeslot-range</td>
<td>• timeslot-range — Specifies the timeslots range from 1 to 24.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router (config-ctrlr-sts1)# vtg 1 t1 1 cem-group 1 timeslots 1-10</td>
</tr>
</tbody>
</table>
## Configuring CEM (SDH Framing)

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `controller sonet-acr acr_no`
4. `framing sdh`
5. `aug mapping au-4`
6. `au-4 au-4-number tug-3 tug-3-number`
7. Do one of the following:
   - `tug-2 tug-2 number e1 e1-line-number cem-group group number timeslots timeslot-range`
8. `exit`

### 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>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>controller sonet-acr acr_no</code></td>
<td>Selects the virtual controller to configure and enters controller configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Access Circuit Redundancy

#### Configuring CEM (SDH Framing)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router (config)# controller sonet-acr 1</td>
<td><em>acr_no—A group number that is valid between 1 and 96. Any group number exceeding this range is not supported.</em></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>framing sdh</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables SDH framing for STM rates.</td>
</tr>
<tr>
<td>Router (config-controller)# framing sdh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>aug mapping au-4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Selects AU-4 Administrative Unit Group (AUG) mapping.</td>
</tr>
<tr>
<td>Router (config-controller)# aug mapping au-4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>au-4 au-4-number tug-3 tug-3-number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.</td>
</tr>
<tr>
<td>Router (config-controller)# au-4 1 tug-3 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• tug-2 tug-2 number e1 e1-line-number cem-group group number timeslots timeslot-range</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Creates a CEM group for the AU-4. Valid E1 values are from 1 to 3.</td>
</tr>
<tr>
<td>Router (config-controller)# tug-2 1 e1 2 cem-group 1 timeslots 1-8</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>tug-2 tug-2 number e1 e1-line-number cem-group group number unframed</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router (config-controller)# tug-2 1 e1 2 cem-group 1 unframed</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Access Circuit Redundancy

### Configuring ATM-ACR on ATM VC Interface for SDH Mode

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `controller sonet-acr acr_no`
4. `au-4 au-4-number tug-3 tug-3-number`
### 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>• 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><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> controller sonet-acr acr_no</td>
<td>Configures ACR controller level.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (config)# controller sonet-acr 1</td>
<td>• acr_no — Specifies the controller unit number.</td>
</tr>
<tr>
<td><strong>Step 4</strong> au-4 au-4-number tug-3 tug-3-number</td>
<td>Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (config-controller)# au-4 1 tug-3 2</td>
<td>• au-4 — Specifies administrative unit</td>
</tr>
<tr>
<td></td>
<td>• au-4-number — A number in the range of 1 to 3.</td>
</tr>
<tr>
<td></td>
<td>• tug-3 — Specifies tributary unit group</td>
</tr>
<tr>
<td></td>
<td>• tug-3-number — A number in the range of 1 to 7.</td>
</tr>
<tr>
<td><strong>Step 5</strong> tug-2 tug-2 number e1 e1-line-number atm</td>
<td>Creates a group for the AU-4. Valid E1 values are from 1 to 3.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (config-controller)# tug-2 1 e1 2 atm</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> interface atm-acr atm-acr-interface-number</td>
<td>Configures the ATM-ACR interface level.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (config)# interface atm-acr 1.1/1/1/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> pvc vpi/vpc</td>
<td>Configures a PVC for the interface and assigns the PVC a VPI and VCI. Do not specify 0 for both the VPI and VCI.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (config-if)# pvc 1/99 l2transport</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring ATM-ACR on ATM VC Interface for SONET Mode

#### SUMMARY STEPS

1. enable
2. configure terminal
3. controller sonet-acr acr_no
4. sts-1 number
5. vtg vtg-number t1 t1-line-number atm
6. interface atm-acr atm-acr-interface-number
7. pvc vpi/vc
8. xconnect peer-router-id vcid encapsulation mpls
9. exit

#### 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></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Configuring Access Circuit Redundancy

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Step 2**

configure terminal  
**Example:**  
Router# configure terminal

**Step 3**

controller sonet-acr acr_no  
**Example:**  
Router (config)# controller sonet-acr 1

**Step 4**

sts-1 number  
**Example:**  
Router (config-controller)# sts-1 1

**Step 5**

vtg vtg-number t1 t1-line-number atm  
**Example:**  
Router (config-ctrlr-sts1)# vtg 1 t1 1 atm

**Step 6**

interface atm-acr atm-acr-interface-number  
**Example:**  
Router (config)# interface atm-acr 1.1/1/1

**Step 7**

pvc vpi/vpc  
**Example:**  
Router (config-if)# pvc 1/99 l2transport

**Step 8**

xconnect peer-router-id vcid encapsulation mpls  
**Example:**  
Router (config-if)# xconnect 2.2.2.2 15 encapsulation mpls

**Step 9**

exit  
**Example:**  
Router (config-if)# exit
What to do next

The following example show ACR virtual interface for ATM PVC in SR-APS environment

Router(config)# controller SONET-ACR 10
Router(config-controller)# sts-1 1
Router(config-ctrlr-tug3)# vtg 1 e1 1 atm
Router(config)# interface atm-acr1.1/1
Router(config-if)# pvc 1/99 l2transport
Router(config-if)# xconnect 2.2.2.2 15 encapsulation mpls
Router(config-if)# exit

Verifying ACR Configurations

This section includes show commands for ACR:

The following example shows the acr groups that have been configured or deleted:

Router# show acr group
ACR Group  Working I/f  Protect I/f  Currently Active  Status
----------------------------------------
1  SONET 4/1/0  SONET 3/1/0  SONET 4/1/0

The following example shows the configured working and protect cem interfaces under the ACR controller:

Router# show acr group 1 detail cem
ACR Group  Working I/f  Protect I/f  Currently Active  Status
----------------------------------------
CE1  CEM4/1/0  CEM3/1/0  CEM4/1/0

Example of a configuration using CESoP:

Router# show running-config | sec SONET-ACR 1
controller SONET-ACR 1
framing sdh
aug mapping au-4
  !
  au-4 1 tug-3 1
  tug-2 1 e1 1 cem-group 0 timeslots 1-31
Example of a configuration using SAToP:

Router# show running-config | sec SONET-ACR 2
controller SONET-ACR 2
framing sdh
aug mapping au-4
  !
  au-4 1 tug-3 1
  tug-2 1 e1 1 cem-group 1001 unframed

The following example shows the loopback ip address for the router:

Router# show ip interface brief | i Loopback
Loopback0  22.22.22.22  YES NVRAM up up

The following example shows the cem-acr circuit status:

Router# show cem circuit
CEM Int.  ID  Ctrlr  Admin  Circuit  AC
----------------------------------------
CEM-ACR1  1  UP  UP  Active  UP
CEM-ACR1  2  UP  UP  Active  UP
CEM-ACR1  3  UP  UP  Active  UP
CEM-ACR1  4  UP  UP  Active  UP
CEM-ACR1  5  UP  UP  Active  UP
CEM-ACR1  6  UP  UP  Active  UP
The following examples show the cem-acr circuit details for cem-group 0 under the CEM-ACR interface:

```
Router# show cem circuit int cem-acr 1 0
CEM-ACR1, ID: 0, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, T1/E1 state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 8 (In use: 0)
Payload Size: 32
Framing: Framed (DS0 channels: 1)
CEM Defects Set
None
Signalling: No CAS
RTP: No RTP
Ingress Pkts: 774186 Dropped: 0
Egress Pkts: 774187 Dropped: 0
CEM Counter Details
Input Errors: 0 Output Errors: 0
Pkts Missing: 0 Pkts Reordered: 0
Misorder Drops: 0 JitterBuf Underrun: 0
Error Sec: 0 Severly Error Sec: 0
Unavailable Sec: 0 Failure Counts: 0
Pkts Malformed: 0 JitterBuf Overrun: 0
```

The following examples show the cem-acr circuit details for cem-group 1001 under the CEM-ACR interface:

```
Router# show cem circuit int cem-acr 1 1001
CEM-ACR1, ID: 1001, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, T1/E1 state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 256
Framing: Unframed
CEM Defects Set
None
Signalling: No CAS
RTP: No RTP
Ingress Pkts: 3096748 Dropped: 0
Egress Pkts: 3096748 Dropped: 0
CEM Counter Details
Input Errors: 0 Output Errors: 0
Pkts Missing: 0 Pkts Reordered: 0
Misorder Drops: 0 JitterBuf Underrun: 0
Error Sec: 0 Severly Error Sec: 0
Unavailable Sec: 0 Failure Counts: 0
Pkts Malformed: 0 JitterBuf Overrun: 0
```

The following example shows the mpls l2 transport vc details for the specified vc. In this case it is the vc with vc-id = 1001:

```
Router# show mpls l2 vc 1001 det
Local interface: CE1 up, line protocol up, CESoPSN Basic 0 up
Destination address: 66.66.66.66, VC ID: 1001, VC status: up
Output interface: Te0/2/0, imposed label stack {1629}
Preferred path: not configured
Default path: active
Next hop: 61.1.1.2
Create time: 03:28:57, last status change time: 03:27:37
Last label FSM state change time: 00:51:41
Signaling protocol: LDP, peer 66.66.66.66:0 up
Targeted Hello: 22.22.22.22(LDP Id) -> 66.66.66.66, LDP is UP
```
Graceful restart: configured and enabled
Non stop routing: not configured and not 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 586, remote 1629
Group ID: local 0, remote 0
MTU: local 0, remote 0
Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  SSO Descriptor: 66.66.66.66/1001, local label: 586
Dataplane:
  SSM segment/switch IDs: 1410842/2339386 (used), FWID: 571
  VC statistics:
    transit packet totals: receive 3119684, send 3112390
    transit byte totals: receive 155984200, send 130720380
    transit packet drops: receive 0, seq error 0, send 0

The following example shows the mpls l2 transport vc details for the specified vc. In this case it is the vc with vc-id = 5001:

Router# show mpls l2 vc 5001 det
Local interface: CE1 up, line protocol up, SATOP E1 1001 up
Destination address: 66.66.66.66, VC ID: 5001, VC status: up
  Output interface: Te0/2/0, imposed label stack {1613}
  Preferred path: not configured
  Default path: active
  Next hop: 61.1.1.2
Create time: 03:29:05, last status change time: 03:27:45
  Last label FSM state change time: 00:51:49
  Signaling protocol: LDP, peer 66.66.66.66:0 up
  Targeted Hello: 22.22.22.22 (LDP Id) -> 66.66.66.66, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not 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 865, remote 1613
Group ID: local 0, remote 0
MTU: local 0, remote 0
Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  SSO Descriptor: 66.66.66.66/1001, local label: 865
Dataplane:
SSM segment/switch IDs: 2176983/3482449 (used), PWID: 850
VC statistics:
- transit packet totals: receive 12488973, send 12445403
- transit byte totals: receive 3347044764, send 3285586392
- transit packet drops: receive 0, seq error 0, send 0

The following example shows the currently configured APS groups on the router:

```
Router# show aps
SONET 0/5/2 APS Group 25: protect channel 0 (Inactive) (HA)
  Working channel 1 at 1.1.1.1 (Enabled) (HA)
  bidirectional, non-revertive
  PGP timers (extended for HA): hello time=1; hold time=10
     hello fail revert time=120
  SDH framing; SDH MSP signalling by default
  Received K1K2: 0x00 0x05
     No Request (Null)
  Transmitted K1K2: 0x00 0x00
     No Request (Null)
  Remote APS configuration: (null)
SONET 0/0/2 APS Group 25: working channel 1 (Active) (HA)
  Protect at 1.1.1.1
  PGP timers (from protect): hello time=1; hold time=10
  SDH framing
  Remote APS configuration: (null)
```

The following example shows ATM ACR configuration on the router:

```
Router# show running-config | sec ACR
controller SONET-ACR 1
  framing sdh
  aug mapping au-4
  
  au-4 1 tug-3 1
     mode c-12
     tug-2 1 e1 1 atm
  
  au-4 1 tug-3 2
     mode c-12
  
  au-4 1 tug-3 3
     mode c-12
  
interface ATM-ACR1.1/1/1
  no ip address
  pvp 1/99 l2transport
  xconnect 51.1.1.2 3 encapsulation mpls
```

The following example shows ATM ACR interfaces on the router:

```
Router# show interface ATM0/1/1.1/1/1 | in pac
  5 minute input rate 4000 bits/sec, 10 packets/sec
  5 minute output rate 4000 bits/sec, 10 packets/sec
  3000 packets input, 156000 bytes, 0 no buffer
  3000 packets output, 156000 bytes, 0 underruns
Router# show xconnect all
Legend: 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
---------------------------------------------------------------------
PN pri ac AT1.1/1/1:10/10(ATM AAL5) UP mpls 3.3.3.3:1 UP
```

Cisco ASR 900 Router Series Configuration Guide, Cisco IOS XE Release 3S
Troubleshooting the ACR configuration

This section provides the supported debug commands to troubleshoot the ACR configuration:

We suggest you do not use these debug commands without TAC supervision.

- **debug acr events**: Provides details on all events occurring on the ACR interface.
- **debug acr errors**: Provides debugging information on errors.
- **debug acr state**: Provides debugging information on state change – when there is a switchover.
- **debug cem events**: Provides debugging information to create and delete CEM circuits.
- **debug cem errors**: Provides debugging information about possible errors while creating and deleting of CEM circuits.
- **debug cem states**: Debugs to show the state changes of CEM circuits.
- **debug atm events**: Provides details on all events occurring on the ATM interface
- **debug atm error**: Provides debugging information on errors.
- **debug atm state**: Provides debugging information on state change – when there is a switchover.

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>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</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>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation 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>
IEEE 802.1Q encapsulation 119, 132
configuration (example) 132
interface 110, 120, 121, 130
basic configuration (example) 130
enabling 110
restarting 120
shutting down 120
verifying configuration 121
interface address, specifying 112
interface configuration mode, summary of 1
interface gigabitethernet command 110
ip address command 110

keyboard shortcuts 8

Management Ethernet Interface, common tasks 135
Management Ethernet interface, interface numbering 133
Management Ethernet interface, IP Address Handling 134
Management Ethernet interface, overview 133
Management Ethernet Interface, VRF 134
modem, accessing 8
modes 1
See command modes 1
mpls mtu command 115
MTU (maximum transmission unit) 114, 115, 116, 131
configuration (example) 131
default size 114
interface MTU 114, 115, 116
additional overhead 115
configuration guidelines 115
configuring 116
description 114
verifying 116
IP MTU, description 114
maximum size 114
types 114
mtu command 110, 116

negotiation auto command 119
no negotiation auto command 120
no shut command 110
NVRAM 120

OIR (online insertion and removal) 120
and shuttering down or restarting interfaces 120
online insertion and removal. See OIR. 120

platforms, supported 17
release notes, identify using 17
privileged EXEC mode, summary of 1
prompts, system 1

question mark (?) command 9

release notes 17
See platforms, supported 17
ROM monitor mode, summary of 1
running configuration, saving to NVRAM 120

SDH mode, configuring 161, 165
Secure Shell (SSH), configuring persistent SSH 25
Secure Shell (SSH), persistent 20
Secure Shell (SSH), persistent SSH restrictions 32
Secure Shell (SSH), viewing handling configuration 29
show history command 9
show hw-module subslot transceiver idprom command 122
show interfaces gigabitethernet command 116
show standby command 114
shutdown command 120
SNAP (Subnetwork Access Protocol) encapsulation 114
Structure-agnostic TDM over PacketStructure-agnostic TDM over Packet (SaToP) 223

T1/E1 Interface Module 139, 140, 143, 156, 199
configuring 140
framing 143
verifying the configuration 156
Tab key, command completion 9
telnet, configuring persistent telnet 23
telnet, persistent 20
telnet, persistent telnet restrictions 32
telnet, using 6
telnet, using to access console 6
telnet, viewing handling configuration 29
Tracing, how tracing works 328
Tracing, overview 327
Tracing, setting a tracing level 331
Tracing, tracing levels 328
Tracing, viewing a tracing level 329
Tracing, viewing trace logs 331
U
user EXEC mode, summary of  1

V
VLANs (virtual LANs)  132
  configuration (example)  132
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

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

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

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

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

© 2017 Cisco Systems, Inc. All rights reserved.