CONTENTS

Preface xiii
Objectives xiii
Organization xiii
Related Documentation xiv
Document Conventions xiv
Obtaining Documentation and Submitting a Service Request xvi

CHAPTER 1

Using Cisco IOS XE Software 1-1
Understanding Command Modes 1-1
Understanding Diagnostic Mode 1-3
Accessing the CLI Using a Console 1-4
    Accessing the CLI Using a Directly-Connected Console 1-4
    Connecting to the Console Port 1-4
    Using the Console Interface 1-5
    Accessing the CLI from a Remote Console Using Telnet 1-6
    Preparing to Connect to the Router Console Using Telnet 1-6
    Using Telnet to Access a Console Interface 1-6
    Accessing the CLI from a Remote Console Using a Modem 1-7
Using the Auxiliary Port 1-7
Using Keyboard Shortcuts 1-8
Using the History Buffer to Recall Commands 1-8
Getting Help 1-8
    Finding Command Options Example 1-9
Using the no and default Forms of Commands 1-12
Saving Configuration Changes 1-12
Managing Configuration Files 1-12
Filtering Output from the show and more Commands 1-14
Powering Off the Router 1-14
Finding Support Information for Platforms and Cisco Software Images 1-14
    Using Cisco Feature Navigator 1-15
    Using Software Advisor 1-15
    Using Software Release Notes 1-15
CHAPTER 2

Console Port, Telnet, and SSH Handling  2-1
   Console Port Overview for the Cisco ASR 900 Series Router  2-1
   Connecting Console Cables  2-1
   Installing USB Device Drivers  2-1
   Console Port Handling Overview  2-2
   Telnet and SSH Overview for the Cisco ASR 900 Series Router  2-2
   Persistent Telnet and Persistent SSH Overview  2-2
   Configuring a Console Port Transport Map  2-3
      Examples  2-5
   Configuring Persistent Telnet  2-5
      Prerequisites  2-5
      Examples  2-7
   Configuring Persistent SSH  2-8
      Examples  2-10
   Viewing Console Port, SSH, and Telnet Handling Configurations  2-11
   Important Notes and Restrictions  2-16

CHAPTER 3

Using the Management Ethernet Interface  3-1
   Gigabit Ethernet Management Interface Overview  3-1
   Gigabit Ethernet Port Numbering  3-1
   IP Address Handling in ROMmon and the Management Ethernet Port  3-2
   Gigabit Ethernet Management Interface VRF  3-2
   Common Ethernet Management Tasks  3-3
      Viewing the VRF Configuration  3-3
      Viewing Detailed VRF Information for the Management Ethernet VRF  3-4
      Setting a Default Route in the Management Ethernet Interface VRF  3-4
      Setting the Management Ethernet IP Address  3-4
      Telnetting over the Management Ethernet Interface  3-4
      Pinging over the Management Ethernet Interface  3-5
      Copy Using TFTP or FTP  3-5
      NTP Server  3-5
      SYSLOG Server  3-5
      SNMP-related services  3-6
      Domain Name Assignment  3-6
      DNS service  3-6
      RADIUS or TACACS+ Server  3-6
      VTY lines with ACL  3-6
CHAPTER 4

High Availability Overview 4-1

Hardware Redundancy Overview 4-1
Stateful Switchover 4-2
SSO-Aware Protocol and Applications 4-2
Bidirectional Forwarding Detection 4-3

CHAPTER 5

Installing and Upgrading Software 5-1

Software Packaging on the Cisco ASR 903 Series Router 5-1
Software Package Modes 5-1
Understanding Cisco ASR 903 Series Router Software Packages 5-2
Provisioning Files 5-2
File Systems on the Cisco ASR 903 Series Router 5-2
System Requirements 5-3
RP Memory Recommendations 5-3
ROMMON Version Requirements 5-4
Determining the Software Version 5-4
Cisco IOS XE 3S to Cisco IOS Version Number Mapping 5-4
Autogenerated Files and Directories 5-5
Setting the Router to Boot in Sub-Package Mode 5-5
Understanding In-Service Software Upgrades 5-6
General Prerequisites for ISSU Upgrade 5-7
Bootflash Space Requirements 5-7
General Restrictions for ISSU Upgrade 5-7
Single-Command ISSU Upgrade 5-7
Restrictions for Single Command ISSU 5-7
Step-By-Step ISSU Upgrade 5-8
Restrictions for Step-By-Step Upgrade 5-8
Downloading an Image 5-8
Completing a Single Command Software Upgrade 5-8
Preparing for Installation 5-8
Completing the Single Command Upgrade 5-9
Performing Step-by-Step ISSU Upgrade 5-10
Upgrading the ROMMON on the RSP Module 5-11
Verifying the Upgrade 5-12
Software Upgrade Examples 5-12
Single Command Software Upgrade 5-12
CHAPTER 8

Configuring T1/E1 Interfaces 8-1

Configuration Tasks 8-1

Limitations 8-1

Required Configuration Tasks 8-2

Setting the Card Type 8-2

Configuring the Controller 8-3

Verifying Controller Configuration 8-4

Optional Configurations 8-4

Configuring Framing 8-5

Setting an IP Address 8-6

Configuring Encapsulation 8-6

Configuring the CRC Size for T1 Interfaces 8-8

Configuring a Channel Group 8-9

Saving the Configuration 8-10

Troubleshooting E1 and T1 Controllers 8-10

Setting Loopbacks 8-10

Running Bit Error Rate Testing 8-12

Monitoring and Maintaining the T1/E1 Interface Module 8-14

Verifying the Interface Configuration 8-14

Verifying Per-Port Interface Status 8-14

Configuration Examples 8-15

Example: Framing and Encapsulation Configuration 8-15

Example: CRC Configuration 8-15

Example: Facility Data Link Configuration 8-16

Example: Invert Data on the T1/E1 Interface 8-16

CHAPTER 9

Enabling Support for Tunable DWDM-XFP-C 9-1

Configuring the DWDM-XFP-C Module 9-3

Verifying the ITU Configuration 9-4

CHAPTER 10

Configuring Optical Interface Modules 10-1

Limitations and Restrictions 10-1

Configuring the Controller 10-2

Configuring SDH 10-2

Configuring SDH Mode 10-3

Configuring SDH in POS Mode 10-5

Configuring SONET Mode 10-6

Configuring SONET Mode 10-6
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SONET POS Mode</td>
<td>10-8</td>
</tr>
<tr>
<td>Configuring a CEM group</td>
<td>10-9</td>
</tr>
<tr>
<td>Configuring CEM Group in SONET Mode</td>
<td>10-9</td>
</tr>
<tr>
<td>Configuring CEM Group in SDH Mode</td>
<td>10-11</td>
</tr>
<tr>
<td>Configuring DS3 Clear Channel on OC-3 and OC-12 Interface Module</td>
<td>10-13</td>
</tr>
<tr>
<td>Configuring DS3 Clear Channel in SONET Mode</td>
<td>10-13</td>
</tr>
<tr>
<td>Configuring DS3 Clear Channel in SDH Mode</td>
<td>10-14</td>
</tr>
<tr>
<td>Optional Configurations</td>
<td>10-16</td>
</tr>
<tr>
<td>Configuring the Encapsulation Method</td>
<td>10-16</td>
</tr>
<tr>
<td>Configuring the CRC Size for T1</td>
<td>10-17</td>
</tr>
<tr>
<td>Optional Packet over SONET Configurations</td>
<td>10-17</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>10-17</td>
</tr>
<tr>
<td>MTU Value</td>
<td>10-18</td>
</tr>
<tr>
<td>CRC Value</td>
<td>10-18</td>
</tr>
<tr>
<td>Keepalive Value</td>
<td>10-18</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>10-18</td>
</tr>
<tr>
<td>Scrambling</td>
<td>10-18</td>
</tr>
<tr>
<td>C2 Flag</td>
<td>10-19</td>
</tr>
<tr>
<td>J1 Flag</td>
<td>10-19</td>
</tr>
<tr>
<td>Managing Interface Naming</td>
<td>10-19</td>
</tr>
<tr>
<td>Identifying Slots and Subslot</td>
<td>10-19</td>
</tr>
<tr>
<td>Configuring Multilink Point-to-Point Protocol</td>
<td>10-20</td>
</tr>
<tr>
<td>MLPPP Configuration Guidelines</td>
<td>10-20</td>
</tr>
<tr>
<td>Creating a Multilink Bundle</td>
<td>10-20</td>
</tr>
<tr>
<td>Assigning an Interface to a Multilink Bundle</td>
<td>10-21</td>
</tr>
<tr>
<td>Configuring Fragmentation Size and Delay on a MLPPP Bundle</td>
<td>10-21</td>
</tr>
<tr>
<td>Changing the Default Endpoint Discriminator</td>
<td>10-22</td>
</tr>
<tr>
<td>Disabling Fragmentation on an MLPPP Bundle</td>
<td>10-22</td>
</tr>
<tr>
<td>Configuring BERT</td>
<td>10-22</td>
</tr>
<tr>
<td>Configuring Automatic Protection Switching</td>
<td>10-22</td>
</tr>
<tr>
<td>Verifying Interface Configuration</td>
<td>10-23</td>
</tr>
<tr>
<td>Verifying Per-Port Interface Status</td>
<td>10-23</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>10-23</td>
</tr>
<tr>
<td>Configuration Examples</td>
<td>10-24</td>
</tr>
<tr>
<td>Example of Cyclic Redundancy Check Configuration</td>
<td>10-24</td>
</tr>
<tr>
<td>Example of Facility Data Link Configuration</td>
<td>10-24</td>
</tr>
<tr>
<td>Example of Invert Data on T1/E1 Interface</td>
<td>10-24</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>10-25</td>
</tr>
</tbody>
</table>
CHAPTER 11
Configuring Clocking and Timing 11-1
Clocking and Timing Restrictions 11-1
Clocking and Timing Overview 11-3
Understanding PTP 11-3
Telecom Profiles 11-4
PTP Redundancy 11-4
Hybrid Clocking 11-5
Transparent Clocking 11-5
Time of Day (TOD) 11-5
Timing Port Specifications 11-6
BITS Framing Support 11-6
Understanding Synchronous Ethernet ESMC and SSM 11-6
Clock Selection Modes 11-7
Managing Clock Selection 11-7
Configuring Clocking and Timing 11-7
Configuring an Ordinary Clock 11-8
Configuring a Master Ordinary Clock 11-8
Configuring a Slave Ordinary Clock 11-11
Configuring a Boundary Clock 11-14
Configuring a Transparent Clock 11-16
Configuring a Hybrid Clock 11-17
Configuring a Hybrid Boundary Clock 11-17
Configuring a Hybrid Ordinary Clock 11-21
Configuring PTP Redundancy 11-24
Configuring PTP Redundancy in Slave Clock Mode 11-24
Configuring PTP Redundancy in Boundary Clock Mode 11-26
Synchronizing the System Time to a Time-of-Day Source 11-28
Synchronizing the System Time to a Time-of-Day Source (Master Mode) 11-28
Synchronizing the System Time to a Time-of-Day Source (Slave Mode) 11-29
Configuring Synchronous Ethernet ESMC and SSM 11-30
Configuring Synchronous Ethernet ESMC and SSM 11-30
Managing Clock Source Selection 11-35
Verifying the Configuration 11-37
Troubleshooting 11-38
Configuration Examples 11-39

CHAPTER 12
Configuring Pseudowire 12-1
Pseudowire Overview 12-1
Circuit Emulation Overview 12-1
Contents

Structure-Agnostic TDM over Packet 12-2
Circuit Emulation Service over Packet-Switched Network 12-3
Asynchronous Transfer Mode over MPLS 12-4
Transportation of Service Using Ethernet over MPLS 12-5

Configuring CEM 12-5
   Configuration Guidelines and Restrictions 12-6
   Configuring a CEM Group 12-6
   Using CEM Classes 12-7
   Configuring CEM Parameters 12-8
      Configuring Payload Size (Optional) 12-8
      Setting the Dejitter Buffer Size 12-9
      Setting an Idle Pattern (Optional) 12-9
      Enabling Dummy Mode 12-9
      Setting a Dummy Pattern 12-9
      Shutting Down a CEM Channel 12-9

Configuring ATM 12-10
   Configuring a Clear-Channel ATM Interface 12-10
   Configuring ATM IMA 12-10
   Configuring Structure-Agnostic TDM over Packet (SAToP) 12-13
   Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN) 12-14
   Configuring a Clear-Channel ATM Pseudowire 12-15
   Configuring an ATM over MPLS Pseudowire 12-16
      Configuring the Controller 12-16
      Configuring an IMA Interface 12-17
      Configuring the ATM over MPLS Pseudowire Interface 12-18
         Configuring 1-to-1 VCC Cell Transport Pseudowire 12-18
         Configuring N-to-1 VCC Cell Transport Pseudowire 12-20
            Configuring 1-to-1 VPC Cell Transport 12-20
            Configuring ATM AAL5 SDU VCC Transport 12-21
            Configuring a Port Mode Pseudowire 12-22
      Optional Configurations 12-23
   Configuring an Ethernet over MPLS Pseudowire 12-23
   Configuring Pseudowire Redundancy 12-25
   Verifying the Interface Configuration 12-27
   Configuration Examples 12-28
      Example: CEM Configuration 12-28
      Example: ATM IMA Configuration 12-28
      Example: ATM over MPLS 12-29
**Cell Packing Configuration Examples** 12-29
**Cell Relay Configuration Examples** 12-33
**Example: Ethernet over MPLS** 12-36

## Chapter 13

### Quality of Service Configuration Guidelines 13-1

- **New and Changed Information** 13-1
- **Understanding Quality of Service** 13-2
- **Configuring Quality of Service** 13-3
- **QoS Support Overview** 13-3
- **QoS Limitations and Guidelines** 13-4
- **Global QoS Limitations** 13-4
  - QoS Features Using MQC Limitations 13-5
  - Etherchannel QoS Limitations 13-5
  - Routed Port-Channel 13-7
  - Restrictions for Hierarchical Policies 13-10
  - MPLS VPN QoS Mapping 13-11
  - QoS Policer and Shaper Calculation 13-12
- **Implementing MPLS Diffserv Tunneling Modes** 13-12
- **Classification** 13-14
  - Ingress Classification Limitations 13-16
  - Egress Classification Limitations 13-16
  - Additional Classification Limitations 13-16
  - Classifying Traffic using an Access Control List 13-16
  - Configuring Multiple match Statements 13-18
  - Classifying Traffic Using Match EFP Service Instance Feature 13-18
- **Marking** 13-20
  - Marking Overview 13-22
  - Ingress Marking Limitations 13-22
  - Egress Marking Limitations 13-22
  - Marking IPv6 Traffic 13-23
  - Additional Marking Limitations 13-23
- **Policing** 13-24
  - Ingress Policing Limitations 13-27
  - Egress Policing Limitations 13-27
- **Shaping** 13-29
  - Additional Shaping Limitations 13-30
- **Congestion Management** 13-30
  - Ingress Queuing Limitations 13-32
  - Egress Queuing Limitations 13-32
Support for Low Latency Queuing on Multiple EFPs 13-33
Additional Queuing Limitations 13-33
Congestion Avoidance 13-33
  Configuring Congestion Avoidance 13-35
  Ingress Congestion Avoidance Limitations 13-36
  Egress Congestion Avoidance Limitations 13-36
  Additional Congestion Avoidance Limitations 13-37
Scheduling 13-38
  Ingress Scheduling Limitations 13-38
  Egress Scheduling Limitations 13-38

CHAPTER 14
Tracing and Trace Management 14-1
  Tracing Overview 14-1
  How Tracing Works 14-1
  Tracing Levels 14-2
  Viewing a Tracing Level 14-3
  Setting a Tracing Level 14-4
  Viewing the Content of the Trace Buffer 14-5

INDEX
Preface

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services. This preface contains the following sections:

- Objectives, page xiii
- Organization, page xiii
- Related Documentation, page xiv
- Document Conventions, page xiv
- Obtaining Documentation and Submitting a Service Request, page xvi

Objectives

This document provides an overview of software functionality that is specific to the Cisco ASR 900 Series Aggregation Services Routers. It is not intended as a comprehensive guide to all of the software features that can be run using the Cisco ASR 900 Series Aggregation Services Routers, but only the software aspects that are specific to this platform.

Unless otherwise specified the procedures in this document apply to all routers under the Cisco ASR 900 Series Aggregation Services Routers.

For information on general software features that are also available on other Cisco platforms, see the Cisco IOS XE technology guide pertaining to that specific software feature.

Organization

This document contains the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview</td>
<td>Provides an overview of the Cisco ASR 900 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>2</td>
<td>Using Cisco IOS XE Software</td>
<td>Provides an introduction to accessing the command-line interface (CLI) and using the Cisco software and related tools.</td>
</tr>
</tbody>
</table>
Chapter Related Documentation

This section refers you to other documentation for configuring your Cisco ASR 900 Series Aggregation Services Routers.

The documentation homepage for the Cisco ASR 900 Series Aggregation Services Routers is:

The documentation homepage for Cisco IOS XE contains Cisco IOS XE technology guides and feature documentation and can be viewed at:

For information on commands, see one of the following resources:

- *Cisco IOS XE Software Command References*
- *Command Lookup Tool* (cisco.com login required)

Document Conventions

This documentation uses the following conventions:
Command syntax descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive.</td>
</tr>
<tr>
<td>string</td>
<td>A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
</tbody>
</table>

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
</tbody>
</table>

Examples use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screen</td>
<td>Examples of information displayed on the screen are set in Courier font.</td>
</tr>
<tr>
<td>bold screen</td>
<td>Examples of text that you must enter are set in Courier bold font.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Angle brackets enclose text that is not printed to the screen, such as passwords.</td>
</tr>
<tr>
<td>!</td>
<td>An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose default responses to system prompts.</td>
</tr>
</tbody>
</table>

The following conventions are used to attract the attention of the reader:
![Caution](image)

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

![Note](image)

Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Using Cisco IOS XE Software

This chapter provides information to prepare you to configure the Cisco ASR 900 Series Router:

- Understanding Command Modes, page 1-1
- Understanding Diagnostic Mode, page 1-3
- Accessing the CLI Using a Console, page 1-4
- Using the Auxiliary Port, page 1-7
- Using Keyboard Shortcuts, page 1-8
- Using the History Buffer to Recall Commands, page 1-8
- Getting Help, page 1-8
- Using the no and default Forms of Commands, page 1-12
- Saving Configuration Changes, page 1-12
- Managing Configuration Files, page 1-12
- Filtering Output from the show and more Commands, page 1-14
- Powering Off the Router, page 1-14
- Finding Support Information for Platforms and Cisco Software Images, page 1-14

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 1-1 describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Log in.</td>
<td>Router&gt;</td>
<td>Use the logout command.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>From user EXEC mode, use the enable EXEC command.</td>
<td>Router#</td>
<td>To return to user EXEC mode, use the disable command.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>From privileged EXEC mode, use the configure terminal privileged EXEC command.</td>
<td>Router(config)#</td>
<td>To return to privileged EXEC mode from global configuration mode, use the exit or end command.</td>
</tr>
<tr>
<td>Interface configuration</td>
<td>From global configuration mode, specify an interface using an interface command.</td>
<td>Router(config-if)#</td>
<td>To return to global configuration mode, use the exit command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To return to privileged EXEC mode, use the end command.</td>
</tr>
</tbody>
</table>
Understanding Diagnostic Mode

Diagnostic mode is supported on the Cisco ASR 900 Series Router.

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.
- The router was accessed using a Route Switch Processor auxiliary port.

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, accessing the router through the auxiliary port is not useful for customer purposes anyway.
A send break signal (Ctrl-C or Ctrl-Shift-6) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

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

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

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

The diagnostic mode commands are stored in the non-IOS packages on the Cisco ASR 900 Series Router, 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, page 1-4
- Accessing the CLI from a Remote Console Using Telnet, page 1-6
- Accessing the CLI from a Remote Console Using a Modem, page 1-7

For more information about connecting cables to the router, see the Cisco ASR 903 Hardware Installation Guide or the Cisco ASR 902 Hardware Installation Guide.

For information about installing USB devices drivers in order to use the USB console port, see the Cisco ASR 903 Hardware Installation Guide or the Cisco ASR 902 Hardware Installation Guide.

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:
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 on a Cisco ASR 900 Series Router 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:

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:
Press RETURN to get started.

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

Step 3 From user EXEC mode, enter the enable command as shown in the following 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”:
Password: enablepass

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

**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”:

```
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”:

```
unix_host% connect
Password:
```
Chapter 1      Using Cisco IOS XE Software

Using the Auxiliary Port

User Access Verification

Password: \textit{mypass}

\textbf{Note} \hspace{1cm} If no password has been configured, press \textit{Return}.

\textbf{Step 3} \hspace{1cm} From user EXEC mode, enter the \texttt{enable} command as shown in the following example:

\texttt{Router> enable}

\textbf{Step 4} \hspace{1cm} At the password prompt, enter your system password. The following example shows entry of the password called “\texttt{enablepass}”:

Password: \texttt{enablepass}

\textbf{Step 5} \hspace{1cm} When the enable password is accepted, the privileged EXEC mode prompt appears:

\texttt{Router#}

\textbf{Step 6} \hspace{1cm} You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

\textbf{Step 7} \hspace{1cm} To exit the Telnet session, use the \texttt{exit} or \texttt{logout} command as shown in the following example:

\texttt{Router# logout}

\textbf{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 Cisco ASR 900 Series Router 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.

For more information about connecting cables to the router, see the \textit{Cisco ASR 903 Hardware Installation Guide} or the \textit{Cisco ASR 902 Hardware Installation Guide}.

\textbf{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 1-2 lists the keyboard shortcuts for entering and editing commands.

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-B or the Left Arrow key</td>
<td>Move the cursor back one character</td>
</tr>
<tr>
<td>Ctrl-F or the Right Arrow key1</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 1-3 lists the history substitution commands.

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

1. 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 1-4 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><code>abbreviated-command-entry?</code></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><code>abbreviated-command-entry&lt;Tab&gt;</code></td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td><code>?</code></td>
<td>Lists all commands available for a particular command mode.</td>
</tr>
<tr>
<td><code>command ?</code></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 1-5 Finding Command Options**

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router&gt; enable</code></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, <code>Router&gt; to Router#</code>.</td>
</tr>
<tr>
<td><code>Router# 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 <code>Router(config)#</code>.</td>
</tr>
</tbody>
</table>
### Table 1-5 Finding Command Options (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# <code>interface gigabitEthernet ?</code>&lt;br&gt;<code>&lt;0-0&gt;</code> GigabitEthernet interface number&lt;br&gt;<code>&lt;0-1&gt;</code> GigabitEthernet interface number</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. 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. When the <code>&lt;cr&gt;</code> symbol is displayed, you can press <code>Enter</code> to complete the command. You are in interface configuration mode when the prompt changes to <code>Router(config-if)#</code>.</td>
</tr>
<tr>
<td>Router(config)#<code>interface gigabitEthernet 0?</code>&lt;br&gt;<code>.&lt;0-0&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Router(config)#<code>interface gigabitEthernet 0/?</code>&lt;br&gt;<code>&lt;0-5&gt;</code> Port Adapter number</td>
<td></td>
</tr>
<tr>
<td>Router(config)#<code>interface gigabitEthernet 0/0?</code>&lt;br&gt;<code>/&lt;0-23&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Router(config)#<code>interface gigabitEthernet 0/0/0?</code>&lt;br&gt;<code>&lt;0-15&gt;</code> GigabitEthernet interface number</td>
<td></td>
</tr>
<tr>
<td>Router(config)#<code>interface gigabitEthernet 0/0/0</code>&lt;br&gt;<code>&lt;0-23&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ?</td>
<td>Enter <code>?</code> to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.</td>
</tr>
<tr>
<td>Interface configuration commands:</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Interface Internet Protocol config commands</td>
</tr>
<tr>
<td><code>keepalive</code></td>
<td>Enable keepalive</td>
</tr>
<tr>
<td><code>lan-name</code></td>
<td>LAN Name command</td>
</tr>
<tr>
<td><code>llc2</code></td>
<td>LLC2 Interface Subcommands</td>
</tr>
<tr>
<td><code>load-interval</code></td>
<td>Specify interval for load calculation for an interface</td>
</tr>
<tr>
<td><code>locaddr-priority</code></td>
<td>Assign a priority group</td>
</tr>
<tr>
<td><code>logging</code></td>
<td>Configure logging for interface</td>
</tr>
<tr>
<td><code>loopback</code></td>
<td>Configure internal loopback on an interface</td>
</tr>
<tr>
<td><code>mac-address</code></td>
<td>Manually set interface MAC address</td>
</tr>
<tr>
<td><code>mls</code></td>
<td>mls router sub/interface commands</td>
</tr>
<tr>
<td><code>mpoa</code></td>
<td>MPOA interface configuration commands</td>
</tr>
<tr>
<td><code>mtu</code></td>
<td>Set the interface Maximum Transmission Unit (MTU)</td>
</tr>
<tr>
<td><code>netbios</code></td>
<td>Use a defined NETBIOS access list or enable name-caching</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td><code>nrzi-encoding</code></td>
<td>Enable use of NRZI encoding</td>
</tr>
<tr>
<td><code>ntp</code></td>
<td>Configure 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>
### Table 1-5 Finding Command Options (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# <code>ip ?</code></td>
<td>Enter the command that you want to configure for the interface. This example uses the <code>ip</code> command. Enter <code>?</code> to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</td>
</tr>
<tr>
<td>Router(config-if)# <code>ip address ?</code></td>
<td>Enter the command that you want to configure for the interface. This example uses the <code>ip address</code> command. Enter <code>?</code> to display what you must enter next on the command line. In this example, you must enter an IP address or the <code>negotiated</code> keyword. A carriage return (&lt;cr&gt;) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</td>
</tr>
<tr>
<td>Router(config-if)# <code>ip address A.B.C.D</code></td>
<td>Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address. Enter <code>?</code> to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. A &lt;cr&gt; is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</td>
</tr>
<tr>
<td>Router(config-if)# <code>ip address A.B.C.D ?</code></td>
<td>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask. Enter <code>?</code> to display what you must enter next on the command line. In this example, you can enter the <code>secondary</code> keyword, or you can press Enter. A &lt;cr&gt; is displayed; you can press Enter to complete the command, or you can enter another keyword.</td>
</tr>
<tr>
<td>Router(config-if)# <code>ip address A.B.C.D 255.255.255.0 ?</code></td>
<td>In this example, Enter is pressed to complete the command.</td>
</tr>
</tbody>
</table>
Using the no and default Forms of Commands

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

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

Saving Configuration Changes

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

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

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

[OK]
Router#

This task saves the configuration to NVRAM.

Managing Configuration Files

On the Cisco ASR 900 Series Router, 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 Cisco ASR 900 Series Router and is used on several Cisco router platforms.

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

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

Example 1: Copying Startup Configuration File to Bootflash

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Feb 2 2000 13:33:40 +05:30 lost+found
15105 drwx 4096 Feb 2 2000 13:35:07 +05:30 .ssh
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
asr903rspi-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
asr903rspi-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_asr-1002-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 } 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
Serial14/0/0 is up, line protocol is up
Serial14/1/0 is up, line protocol is up
Serial14/2/0 is administratively down, line protocol is down
Serial14/3/0 is administratively down, line protocol is down

Powering Off the Router

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

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

The following screenshot shows an example of this process:

```
Router# reload
Proceed with reload? [confirm]
```


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

Finding Support Information for Platforms and Cisco Software Images

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

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

Using Software Advisor

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

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

Using Software Release Notes

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

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

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. Refer to Cisco Feature Navigator for cumulative feature information.
CHAPTER 2

Console Port, Telnet, and SSH Handling

This chapter covers the following topics:
- Console Port Overview for the Cisco ASR 900 Series Router, page 2-1
- Console Port Handling Overview, page 2-2
- Telnet and SSH Overview for the Cisco ASR 900 Series Router, page 2-2
- Persistent Telnet and Persistent SSH Overview, page 2-2
- Configuring a Console Port Transport Map, page 2-3
- Configuring Persistent Telnet, page 2-5
- Configuring Persistent SSH, page 2-8
- Viewing Console Port, SSH, and Telnet Handling Configurations, page 2-11
- Important Notes and Restrictions, page 2-16

Console Port Overview for the Cisco ASR 900 Series Router

The console port on the Cisco ASR 900 Series Router 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 router and is located on the front panel of the Route Switch Processor (RSP).

For information on accessing the router 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 Cisco ASR 900 Series Router, see the Cisco ASR 903 Hardware Installation Guide or the Cisco ASR 902 Hardware Installation Guide.

Installing USB Device Drivers

For instructions on how to install device drivers in order to use the USB console port, see the Cisco ASR 903 Hardware Installation Guide or the Cisco ASR 902 Hardware Installation Guide.
Console Port Handling Overview

Users using the console port to access the router 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 for the Cisco ASR 900 Series Router

Telnet and Secure Shell (SSH) on the Cisco ASR 900 Series Router 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 Cisco ASR 900 Series Router 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 Cisco ASR 900 Series Router 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” section on page 2-5 and the “Configuring Persistent SSH” section on page 2-8.
Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the Cisco ASR 900 Series Router.

**SUMMARY STEPS**

1. (Required) `enable`
2. (Required) `configure terminal`
3. (Required) `transport-map type console transport-map-name`
4. (Required) `connection wait [allow interruptible | none {disconnect}]`
5. (Optional) `banner [diagnostic | wait] banner-message`
6. (Required) `exit`
7. (Required) `transport type console console-line-number input transport-map-name`
## Configuring a Console Port Transport Map

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</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** transport-map type console transport-map-name | Creates and names a transport map for handling console connections, and enter transport map configuration mode.  |
| **Example:**  
Router(config)# transport-map type console consolehandler | |
| **Step 4** connection wait [allow interruptible | none] | Specifies how a console connection will be handled using this transport map:  
- **allow interruptible**—The console connection waits for an IOS vty line to become available, and also allows user to enter diagnostic mode by interrupting a console connection waiting for the IOS vty line to become available. This is the default setting.  
- **none**—The console connection immediately enters diagnostic mode.  
**Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.  |
| **Example:**  
Router(config-tmap)# connection wait none | |
| **Step 5** banner [diagnostic | wait] banner-message | (Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS vty line as a result of the console transport map configuration.  
- **diagnostic**—Creates a banner message seen by users directed into diagnostic mode as a result of the console transport map configuration.  
- **wait**—Creates a banner message seen by users waiting for the IOS vty to become available.  
- **banner-message**—The banner message, which begins and ends with the same delimiting character.  |
| **Example:**  
Router(config-tmap)# banner diagnostic X  
Enter TEXT message. End with the character 'X'.  
--Welcome to Diagnostic Mode--X  
Router(config-tmap)# | |
### Configuring Persistent Telnet

This task describes how to configure persistent Telnet on the Cisco ASR 900 Series Router.

### Prerequisites

For a persistent Telnet connection to access an IOS vty line on the Cisco ASR 900 Series Router, 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. (Required) `enable`
2. (Required) `configure terminal`
3. (Required) `transport-map type persistent telnet transport-map-name`

### 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'.  
   Welcome to diagnostic mode  
   X  
Router(config-tmap)# banner wait X  
   Enter TEXT message.  End with the character 'X'.  
   Waiting for IOS vty line  
   X  
Router(config-tmap)# exit  

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

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

4. (Required) `connection wait [allow {interruptible} | none {disconnect}]`

5. (Optional) `banner [diagnostic | wait] banner-message`

6. (Required) `transport interface GigabitEthernet 0`

7. (Required) `exit`

8. (Required) `transport type persistent telnet input transport-map-name`

#### Detailed Steps

<table>
<thead>
<tr>
<th>Command</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** transport-map type persistent telnet transport-map-name | Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.  
Example:  
Router(config)# transport-map type persistent telnet telnet handler |
| **Step 4** connection wait [allow {interruptible} | none {disconnect}] | Specifies how a persistent Telnet connection will be handled using this transport map:  
- allow—The Telnet connection waits for an IOS vty line to become available, and exits the router if interrupted.  
- allow interruptible—The Telnet connection waits for the IOS vty line to 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.  
Example:  
Router(config-tmap)# connection wait none |

#### 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.
### Command

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`banner [diagnostic</td>
<td>wait] banner-message`</td>
</tr>
</tbody>
</table>

**Example:**

Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)#

| Step 6 | 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 Cisco ASR 900 Series Router. This step must be taken before applying the transport map to the Management Ethernet interface. |

**Example:**

Router(config-tmap)# transport interface gigabitethernet 0

| Step 7 | exit | Exits transport map configuration mode to re-enter global configuration mode. |

**Example:**

Router(config-tmap)# exit

| Step 8 | transport type persistent telnet input transport-map-name | Applies the settings defined in the transport map to the Management Ethernet interface. The `transport-map-name` for this command must match the `transport-map-name` defined in the `transport-map type persistent telnet` command. |

**Example:**

Router(config)# transport type persistent telnet input telnethandler

### Examples

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

A diagnostic and a wait banner are also configured.

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

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

Configuring Persistent SSH

This task describes how to configure persistent SSH on the Cisco ASR 900 Series Router.

SUMMARY STEPS

1. (Required) enable
2. (Required) configure terminal
3. (Required) transport-map type persistent ssh transport-map-name
4. (Required) connection wait [allow {interruptible} | none {disconnect}]
5. (Required) rsa keypair-name rsa-keypair-name
6. (Optional) authentication-retries number-of-retries
7. (Optional) banner [diagnostic | wait] banner-message
8. (Optional) time-out timeout-interval-in-seconds
9. (Required) transport interface GigabitEthernet 0
10. (Required) exit
11. (Required) transport type persistent ssh input transport-map-name

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>transport-map type persistent ssh transport-map-name</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# transport-map type persistent ssh sshhandler</td>
</tr>
<tr>
<td></td>
<td>Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode.</td>
</tr>
</tbody>
</table>
### Chapter 2  Console Port, Telnet, and SSH Handling

#### Configuring Persistent SSH

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>connection wait [allow (interruptible)</td>
<td>none {disconnect}]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

| Step 5 | rsa keypair-name rsa-keypair-name | Names the RSA keypair to be used for persistent SSH connections. |
|        |         | For persistent SSH connections, the RSA keypair name must be defined using this command in transport map configuration mode. The RSA keypair definitions defined elsewhere on the router, such as through the use of the ip ssh rsa keypair-name command, do not apply to persistent SSH connections. |
|        |         | No rsa-keypair-name is defined by default. |

| Step 6 | authentication-retries number-of-retries | (Optional) Specifies the number of authentication retries before dropping the connection. |
|        |         | The default number-of-retries is 3. |

| Step 7 | banner [diagnostic | wait] banner-message | (Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the vty line as a result of the persistent SSH configuration. |
|        |         | - diagnostic—Creates a banner message seen by users directed into diagnostic mode as a result of the persistent SSH configuration. |
|        |         | - wait—Creates a banner message seen by users waiting for the vty line to become active. |
|        |         | - banner-message—The banner message, which begins and ends with the same delimiting character. |
### Command Purpose

<table>
<thead>
<tr>
<th>Step 8</th>
<th>time-out timeout-interval</th>
<th>(Optional) Specifies the SSH time-out interval in seconds. The default <code>timeout-interval</code> is 120 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config-tmap)# time-out 30</code></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>transport interface gigabitethernet 0</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 Cisco ASR 900 Series Router.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config-tmap)# transport interface gigabitethernet 0</code></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>exit</td>
<td>Exits transport map configuration mode to re-enter global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router(config-tmap)# exit</code></td>
<td></td>
</tr>
<tr>
<td>Step 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 <code>transport-map-name</code> for this command must match the <code>transport-map-name</code> defined in the <code>transport-map type persistent ssh</code> command.</td>
</tr>
<tr>
<td>Example:</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`
Viewing Console Port, SSH, and Telnet Handling Configurations

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

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

Router# `show transport-map all`
Transport Map:
   Name: consolehandler
   Type: Console Transport

Connection:
   Wait option: Wait Allow Interruptable
   Wait banner:

Waiting for the IOS CLI

   bshell banner:

Welcome to Diagnostic Mode

Transport Map:
   Name: sshhandler
   Type: Persistent SSH Transport

Interface:
   GigabitEthernet0

Connection:
   Wait option: Wait Allow Interruptable
   Wait banner:

Waiting for IOS prompt

   Bshell banner:

Welcome to Diagnostic Mode

SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Transport Map:
   Name: telnethandler
   Type: Persistent Telnet Transport

Interface:
   GigabitEthernet0

Connection:
   Wait option: Wait Allow Interruptable
   Wait banner:

Waiting for IOS process
   Bshell banner:

Welcome to Diagnostic Mode

Transport Map:
   Name: telnethandling1
   Type: Persistent Telnet Transport

Connection:
   Wait option: Wait Allow

Router# show transport-map type console
Transport Map:
   Name: consolehandler
   Type: Console Transport

Connection:
   Wait option: Wait Allow Interruptable
   Wait banner:

Waiting for the IOS CLI
   Bshell banner:

Welcome to Diagnostic Mode

Router# show transport-map type persistent ssh
Transport Map:
   Name: sshhandler
   Type: Persistent SSH Transport

Interface:
   GigabitEthernet0

Connection:
   Wait option: Wait Allow Interruptable
   Wait banner:

Waiting for IOS prompt
   Bshell banner:

Welcome to Diagnostic Mode
SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys

Router# **show transport-map type persistent telnet**
Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode

Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport

Connection:
  Wait option: Wait Allow

Router# **show transport-map name telnethandler**
Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode

Router# **show transport-map name consolehandler**
Transport Map:
  Name: consolehandler
  Type: Console Transport

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for the IOS CLI

Bshell banner:
Welcome to Diagnostic Mode

Router# show transport-map name sshhandler
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS prompt
  Bshell banner:

Welcome to Diagnostic Mode

SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys

Router#

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

Router# show platform software configuration access policy
The current access-policies

  Method : telnet
  Rule    : wait
  Shell banner:
  Wait banner :

  Method : ssh
  Rule    : wait
  Shell banner:
  Wait banner :

  Method : console
  Rule    : wait with interrupt
  Shell banner:
  Wait banner :

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

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

Router# show platform software configuration access policy
Chapter 2    Console Port, Telnet, and SSH Handling

Viewing Console Port, SSH, and Telnet Handling Configurations

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:

Method      : console
Rule        : wait with interrupt
Shell 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
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.
Using the Management Ethernet Interface

This chapter covers the following topics:

- Gigabit Ethernet Management Interface Overview, page 3-1
- Gigabit Ethernet Port Numbering, page 3-1
- Gigabit Ethernet Port Numbering, page 3-1
- IP Address Handling in ROMmon and the Management Ethernet Port, page 3-2
- Gigabit Ethernet Management Interface VRF, page 3-2
- Common Ethernet Management Tasks, page 3-3

Gigabit Ethernet Management Interface Overview

The Cisco ASR 900 Series Router 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” section on page 2.

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 telnetted to through the console port, however.

The port can be accessed in configuration mode like any other port on the Cisco ASR 900 Series Router.

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

IP Address Handling in ROMmon and the Management Ethernet Port

On the Cisco ASR 900 Series Router, IP addresses can be configured in ROMmon (the IP_ADDRESS= and IP_SUBNET_MASK= commands) and through the use of the IOS command-line interface (the ip address command in interface configuration mode).

Assuming the IOS process has not begun running on the Cisco ASR 900 Series Router, 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 Cisco ASR 900 Series Router 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 Cisco ASR 900 Series Router 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, page 3-3
- Viewing Detailed VRF Information for the Management Ethernet VRF, page 3-4
- Setting a Default Route in the Management Ethernet Interface VRF, page 3-4
- Setting the Management Ethernet IP Address, page 3-4
- Telnetting over the Management Ethernet Interface, page 3-4
- Pinging over the Management Ethernet Interface, page 3-5
- Copy Using TFTP or FTP, page 3-5
- NTP Server, page 3-5
- SYSLOG Server, page 3-5
- SNMP-related services, page 3-6
- Domain Name Assignment, page 3-6
- DNS service, page 3-6
- RADIUS or TACACS+ Server, page 3-6
- VTY lines with ACL, page 3-6

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
```

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
```
Chapter 3  Using the Management Ethernet Interface

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 IP 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
```
High Availability Overview

Cisco High Availability (HA) enables network-wide protection by providing fast recovery from faults that may occur in any part of the network. With Cisco High Availability, network hardware and software work together and enable rapid recovery from disruptions to ensure fault transparency to users and network applications.

The unique hardware and software architecture of the Cisco ASR 903 Series Router is designed to maximize router uptime during any network event, and thereby provide maximum uptime and resilience within any network scenario.

This chapter covers the aspects of High Availability that are unique to the Cisco ASR 903 Series Router. It is not intended as a comprehensive guide to High Availability, nor is it intended to provide information on High Availability features that are available on other Cisco routers that are configured and implemented identically on the Cisco ASR 903 Series Router. The Cisco IOS feature documents and guides should be used in conjunction with this chapter to gather information about High Availability-related features that are available on multiple Cisco platforms and work identically on the Cisco ASR 903 Series Router.

This section discusses various aspects of High Availability on the Cisco ASR 903 Series Router and contains the following sections:

- Hardware Redundancy Overview, page 4-1
- Stateful Switchover, page 4-2
- Stateful Switchover, page 4-2
- Bidirectional Forwarding Detection, page 4-3

Hardware Redundancy Overview

The Cisco ASR 903 Series Router supports redundant Route Switch Processors (RSPs) and power supplies. Redundancy is not supported on interface modules.

Note

Some interface modules require a reload during a software upgrade, briefly interrupting traffic.

Hardware redundancy provides the following benefits:

- A failover option—If a processor fails, the standby processor immediately becomes the active processor with little or no delay. The failover happens completely within the same router, so a second standby router is not needed.
Stateful Switchover

- No downtime upgrades—Using features like ISSU, a software upgrade can be handled on the standby processor while the active processor continues normal operation.

Table 4-1 provides a hardware redundancy overview.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Support for Dual Hardware Configuration</th>
<th>Failover Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Switch Processor</td>
<td>Yes</td>
<td>If an active RSP experiences an event that makes it unable to forward traffic (such as a hardware failure, a software failure, an OIR, or a manual switch) and a standby RSP is configured, the standby RSP immediately becomes the active RSP.</td>
</tr>
<tr>
<td>Interface module</td>
<td>No</td>
<td>No standby configurations are available for interface modules. If an interface module fails, it cannot forward traffic. In the event of an interface module shutdown, all other interface modules remain fully operational.</td>
</tr>
</tbody>
</table>

Stateful Switchover

The Stateful Switchover (SSO) feature takes advantage of processor redundancy by establishing one of the processors as the active processor while the other RSP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RSP state information between the dual processors.

Stateful Switchover is particularly useful in conjunction with Nonstop Forwarding. SSO allows the dual processors to maintain state at all times, and Nonstop Forwarding lets a switchover happen seamlessly when a switchover occurs.

It is important to note that in most cases, SSO requires less downtime for switchover and upgrades than RPR. RPR should only be used when there is a compelling reason to not use SSO.

For additional information on NSF/SSO, see the Cisco Nonstop Forwarding document.

SSO-Aware Protocol and Applications

SSO-supported line protocols and applications must be SSO-aware. A feature or protocol is SSO-aware if it maintains, either partially or completely, undisturbed operation through an RSP switchover. State information for SSO-aware protocols and applications is synchronized from active to standby to achieve stateful switchover for those protocols and applications.

The dynamically created state of SSO-unaware protocols and applications is lost on switchover and must be reinitialized and restarted on switchover.

To see which protocols are SSO-aware on your router, use the following commands show redundancy client or show redundancy history.
Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier, and reconvergence time is consistent and predictable.

For more information on BFD, see the Release Notes and the IP Routing BFD Configuration Guide, Cisco IOS XE Release 3S.
Installing and Upgrading Software

This chapter describes how to update software on the Cisco ASR 903 Series Router and includes the following sections:

- Software Packaging on the Cisco ASR 903 Series Router, page 5-1
- File Systems on the Cisco ASR 903 Series Router, page 5-2
- System Requirements, page 5-3
- Autogenerated Files and Directories, page 5-5
- Setting the Router to Boot in Sub-Package Mode, page 5-5
- Understanding In-Service Software Upgrades, page 5-6
- Downloading an Image, page 5-8
- Completing a Single Command Software Upgrade, page 5-8
- Performing Step-by-Step ISSU Upgrade, page 5-10
- Upgrading the ROMMON on the RSP Module, page 5-11
- Software Upgrade Examples, page 5-12

Software Packaging on the Cisco ASR 903 Series Router

This section covers the following topics:

- Software Package Modes, page 5-1
- Provisioning Files, page 5-2

Software Package Modes

The Cisco ASR 903 router can be booted using any of the following:

- Consolidated image—A single software image containing a full collection of software packages. Step-By-Step (consolidated mode) ISSU provides a simplified installation and can be stored in bootflash, a TFTP server, or a network server.
- Sub-package—One or more sub-images extracted from the consolidated image. Sub-package mode provides optimized memory usage and requires that you store files in the bootflash directory. The router supports sub-package mode.
Understanding Cisco ASR 903 Series Router Software Packages

Table 5-1 summarizes the sub-packages within a consolidated image.

<table>
<thead>
<tr>
<th>Sub-Package</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPBase</td>
<td>Route Switch Processor (RSP) operating system</td>
</tr>
<tr>
<td>RPControl</td>
<td>Control plane processes between IOS process and the rest of the platform.</td>
</tr>
<tr>
<td>RPAccess</td>
<td>Handles security features including Secure Socket Layer (SSL) and Secure Shell (SSH)</td>
</tr>
<tr>
<td>RPIOS</td>
<td>Cisco IOS kernel, which is where IOS features are stored and run.</td>
</tr>
</tbody>
</table>

Note: Each consolidated image has a unique RPIOS package.

<table>
<thead>
<tr>
<th>Sub-Package</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP Pkg</td>
<td>Controls FP daemons.</td>
</tr>
<tr>
<td>IO Pkg</td>
<td>Controls input/output driver daemons.</td>
</tr>
<tr>
<td>LC Base</td>
<td>Controls basic kernel functions including runtime, initialization scripts, and chassis control daemons.</td>
</tr>
</tbody>
</table>

Provisioning Files

Provisioning files manage the boot process when the Cisco ASR 903 Series Router is configured to boot in sub-packages. The provisioning file manages the bootup of each individual sub-package. Provisioning files are extracted automatically when individual sub-package files are extracted from a consolidated package. Provisioning files are not necessary for running the router using the complete consolidated package.

File Systems on the Cisco ASR 903 Series Router

Table 5-5 provides a list of file systems that can be seen on the Cisco ASR 903 Series Router.

<table>
<thead>
<tr>
<th>File System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash:</td>
<td>The boot flash memory file system on the active RSP.</td>
</tr>
<tr>
<td>cns:</td>
<td>The Cisco Networking Services file directory.</td>
</tr>
<tr>
<td>nvram:</td>
<td>Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.</td>
</tr>
<tr>
<td>stby-bootflash:</td>
<td>The boot flash memory file system on the standby RSP.</td>
</tr>
<tr>
<td>stby-harddisk:</td>
<td>The hard disk file system on the standby RSP.</td>
</tr>
<tr>
<td>stby-usb[0-1]:</td>
<td>The Universal Serial Bus (USB) flash drive file systems on the standby RSP.</td>
</tr>
<tr>
<td>system:</td>
<td>The system memory file system, which includes the running configuration.</td>
</tr>
<tr>
<td>tar:</td>
<td>The archive file system.</td>
</tr>
<tr>
<td>tmpsys:</td>
<td>The temporary system files file system.</td>
</tr>
<tr>
<td>usb[0-1]:</td>
<td>The Universal Serial Bus (USB) flash drive file systems on the active RSP.</td>
</tr>
</tbody>
</table>
If you see a file system not listed in Table 5-5, enter the help option or see the copy command reference for additional information on that file system.

**System Requirements**

The following sections describe the system requirements for the Cisco ASR 903 Series Router software:

- RP Memory Recommendations, page 5-3
- ROMMON Version Requirements, page 5-4
- Determining the Software Version, page 5-4
- Cisco IOS XE 3S to Cisco IOS Version Number Mapping, page 5-4

**RP Memory Recommendations**

Table 3 describes the consolidated package images, individual software sub-package contents, and memory recommendations for each RSP.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Individual Sub-package Contents</th>
<th>DRAM Memory</th>
</tr>
</thead>
</table>
### System Requirements

**ROMMON Version Requirements**

ROMMON Release 15.3(1r)S1 is the recommended release for all ROMMON upgradeable components. For more information about ROMMON images, see Release Notes for the Cisco ASR 903 Router.

**Determining the Software Version**

You can use the `show version installed` command to list the installed sub-packages on the router.

**Cisco IOS XE 3S to Cisco IOS Version Number Mapping**

Each version of Cisco IOS XE 3S has an associated Cisco IOS version. Table 4 lists these mappings for Release 3.50S and forward.

<table>
<thead>
<tr>
<th>Table 4</th>
<th>Cisco IOS XE 3S to Cisco IOS Version Number Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco IOS XE 3S Version</strong></td>
<td><strong>Cisco IOS Version</strong></td>
</tr>
<tr>
<td>3.5.0S</td>
<td>15.2(1)S</td>
</tr>
<tr>
<td>3.5.1S</td>
<td>15.2(1)S1</td>
</tr>
<tr>
<td>3.6.0S</td>
<td>15.2(2)S</td>
</tr>
<tr>
<td>3.6.1S</td>
<td>15.2(2)S1</td>
</tr>
<tr>
<td>3.7.0S</td>
<td>15.2(4)S</td>
</tr>
<tr>
<td>3.8.0S</td>
<td>15.3(1)S</td>
</tr>
<tr>
<td>3.9.0S</td>
<td>15.3(2)S</td>
</tr>
</tbody>
</table>

---

### Table 3

**Memory Recommendations for the Cisco ASR 903 Series Router Consolidated Package Image**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Image Name</th>
<th>Software Image</th>
<th>Individual Sub-package Contents</th>
<th>DRAM Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 903 Router</td>
<td>Cisco ASR 903 Series RSP1 UNIVERSAL NPE</td>
<td>asr903rsp1-universalk9_npe.version.bin</td>
<td>asr903-hw-programmables.version.pkg</td>
<td>2 GB (RSP1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr903rsp1-espbase.version.pkg</td>
<td>4 GB (RSP1+)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr903rsp1-packages-universalk9.version.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr903rsp1-rpaccess.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr903rsp1-rpbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr903rsp1-rpcontrol.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr903rsp1-rpios-universalk9_npe.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr903rsp1-sipbase.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>asr903rsp1-sipspa.version.pkg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>packages.conf</td>
<td></td>
</tr>
</tbody>
</table>
Autogenerated Files and Directories

Table 5-5 provides a list and descriptions of autogenerated files on the Cisco ASR 903 Series Router.

Caution
Do not alter any autogenerated file in the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by customer support; altering these files can have unpredictable consequences for system performance.

Table 5-5 Autogenerated Files

<table>
<thead>
<tr>
<th>File or Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashinfo files</td>
<td>A crashinfo file may appear in the bootflash: file system. Crashinfo files are useful for tuning and troubleshooting, but are not related to router operations: you can erase them without impacting the router’s performance.</td>
</tr>
<tr>
<td>core files</td>
<td>The bootflash/core directory is the storage area for .core files. Caution: Do not erase or move the core directory.</td>
</tr>
<tr>
<td>lost+found directory</td>
<td>This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.</td>
</tr>
<tr>
<td>tracelogs files</td>
<td>The storage area for trace files is bootflash/tracelogs. Trace files are useful for troubleshooting; you can access trace files using diagnostic mode to gather information related to the IOS failure. Caution: Do not erase or move the tracelog directory.</td>
</tr>
</tbody>
</table>

Setting the Router to Boot in Sub-Package Mode

Follow these steps to configure the router to boot in sub-package mode.

Note
For instructions on how to download an image file, see Downloading an Image, page 5-8. In the following example, the image is located in the bootflash: Image/image-name.
Understanding In-Service Software Upgrades

The in-service software upgrade (ISSU) process allows you to update the router software with minimal service interruption.

Starting Cisco IOS XE Release 3.11, ISSU is supported on both sub-package and step-by-step modes on the router.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router# configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Step 2 Router(config)# config-register 0x2</td>
<td>Sets the configuration register so that the router boots using a specified image in NVRAM.</td>
</tr>
<tr>
<td>Step 3 request platform software package expand file source-URL [to destination-URL] [force] [verbose] [wipe]</td>
<td>Expands the consolidated image file on the active RSP.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# request platform software package expand file bootflash:Image/asr903rsp1-adventerprisek9.base.bin</td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 5 Switch to the standby RSP console.</td>
<td></td>
</tr>
<tr>
<td>Step 6 request platform software package expand file source-URL [to destination-URL] [force] [verbose] [wipe]</td>
<td>Expands the consolidated image file on the standby RSP.</td>
</tr>
<tr>
<td></td>
<td>Note This step applies only if your router has a redundant RSP.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# request platform software package expand file stby-bootflash:Image/asr903rsp1-adventerprisek9.base.bin</td>
</tr>
<tr>
<td>Step 7 boot system flash [flash-fs:] [partition-number:] [filename]</td>
<td>Sets the router to boot using the packages.conf file.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# boot system bootflash:Image/packages.conf</td>
</tr>
<tr>
<td>Step 8 exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 9 Router# copy running-config startup-config</td>
<td>Saves the configuration.</td>
</tr>
<tr>
<td>Step 10 Router# reload</td>
<td>Reloads the router.</td>
</tr>
</tbody>
</table>
Note

In Cisco IOS XE Release 3.7 to 3.10, ISSU was not supported using step-by-step mode.

Two types ISSU upgrade is supported on the router.
- Single-Command ISSU Upgrade, page 5-7
- Step-By-Step ISSU Upgrade, page 5-8

General Prerequisites for ISSU Upgrade

- The router must be booted in sub-package mode (with package.conf).
- The package.conf (base image packages) and the upgrade image should exist in the same location in the bootflash.

Bootflash Space Requirements

The in-service software upgrade (ISSU) process requires a minimum of 600 MB available space in bootflash memory.

General Restrictions for ISSU Upgrade

The following restrictions apply when completing an in-service software upgrade on the router.
- ISSU is not supported for single RSP configurations.
- Cisco IOS XE software compatibility is supported only between identical image types. Cross-image-type upgrades or installations (such as from an Universal image to an Universalk9_npeimage) are not supported in the ISSU process.
- Running two different image types simultaneously is not supported.
- ISSU upgrades from one package mode to another are not supported.

Single-Command ISSU Upgrade

A single command upgrade allows you to install a complete set of sub-packages using a single command.

The command installs the complete set of packages on the standby RSP, and then perform a rolling reload of the interface modules on the active RSP. After the interface modules are reloaded, an HA switchover is performed and the complete set of sub-packages will be installed on the new (i.e. previously active) RSP.

For information about completing a single-command upgrade, see Completing a Single Command Software Upgrade, page 5-8.

Restrictions for Single Command ISSU

- TDM interfaces or IM present in the router are reset when ISSU is performed.
- Gigabit Ethernet IM present in the router are reset in the following conditions:
- FGPA version of IM is higher in the new image than the existing FPGA version on the IM which ISSU is being performed.
- Different versions of PHY API is present on the new image.
- Change in PHY API initialization exists in new image causing a PHY reinitialization.

**Step-By-Step ISSU Upgrade**

Starting with Cisco IOS XE Release 3.11S and later releases, step-by-step ISSU upgrade is available on the router.

For information on performing a step-by-step ISSU, see Performing Step-by-Step ISSU Upgrade, page 5-10.

**Restrictions for Step-By-Step Upgrade**

- ISSU is *not* supported if TDM and OC-3 IMs are installed on the router.

**Downloading an Image**

Download the image to the same partition of the bootflash where the base image exists. For information on downloading images see, *Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 903)*.

⚠️ **Caution**

Ensure that you have chosen an upgrade image that is supported by your current software version.

**Completing a Single Command Software Upgrade**

A single command upgrade updates the active and standby RSPs with a single IOS command. Follow these steps to complete the one-shot upgrade.

**Preparing for Installation**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify the chassis is booted using sub-package mode and in hot standby state, else set the router to sub-package mode, see Setting the Router to Boot in Sub-Package Mode, page 5-5.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Download the new consolidated image file from Cisco.com on the chassis. For more information about downloading Cisco software image, see Chapter 1, “Using Cisco IOS XE Software.”</td>
</tr>
<tr>
<td>Step 3</td>
<td>Open a console session to the active RSP. For instructions on how to open a console session, see Console Port, Telnet, and SSH Handling, page 2-1.</td>
</tr>
</tbody>
</table>
### Completing a Single Command Software Upgrade

**Step 4**
Copy the new consolidated image file to the active image bootflash directory such that the new image file is in the same location as the existing image file.

**Note**
Do not copy the packages.conf file to a new directory after expanding the package. It is required that the packages.conf file and sub package files exist in the same directory.

**Note**
It is not necessary to copy the new consolidated image file to the standby RSP; the one-shot upgrade process completes this step.

**Step 5**
**Router# configure terminal**
Enters configuration mode.

**Step 6**
**Router(config)# redundancy**
**Router(config-red)#**
Enters redundancy configuration mode.

**Step 7**
**Router(config-red)# mode sso**
Sets the router in SSO redundancy mode.

**Step 8**
**end**
Exits configuration mode and returns to the EXEC command prompt.

**Example:**
**Router(config)# end**

**Step 9**
```
*Jan 12 17:52:26.516:
%RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
```
Confirms that the router has reached SSO state; wait for this output before proceeding.

**Step 10**
**Router# copy running-config startup-config**
Saves the configuration.

## Completing the Single Command Upgrade

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

- `request platform software package`
- `install node file file-URL`
  `[interface-module-delay delay]`

**Example:**
**Router# request platform software package install node file bootflash:Image/asr903rsp1-adventerp risek9.upgrade.bin interface-module-delay 160**

- Initiates the one-shot installation procedure using the consolidated image file.

  **Note**
  You can adjust the delay between the OIR of each IM using the `interface-module-delay` keyword.

  **Caution**
  We recommend you set the `interface-module-delay` value to 150 seconds or greater in order to ensure sufficient time for IM software upgrades.

  **Note**
  Keywords other than `interface-module-delay` are not supported.

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>The router displays a series of STAGE/SUCCESS messages.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For sample output of a single command upgrade, see Software Upgrade Examples, page 5-12.</td>
</tr>
</tbody>
</table>
Performing Step-by-Step ISSU Upgrade

**Step 1** Verify the chassis is booted using sub-package mode and in hot standby state, else set the router to sub-package mode, see Setting the Router to Boot in Sub-Package Mode, page 5-5.

**Step 2** Download the image on the chassis.

**Step 3** Extract the sub-package images from the asr903rsp1-adventerprisek9.upgrade.bin image on the active RSP using the `request platform software package expand file bootflash:Image/asr903rsp1-adventerprisek9.upgrade.bin` command.

**Step 4** Extract the sub-package image from the asr903rsp1-adventerprisek9.upgrade.bin image on the standby RSP using the `request platform software package expand file stby-bootflash:Image/asr903rsp1-adventerprisek9.upgrade.bin` command.

**Step 5** Upgrade all the sub-packages on the standby RSP using the `request platform software package install rp stdby_slot_num file stby-bootflash:asr903rsp1-*.upgrade.pkg` command.

**Step 6** Reload the standby module from active RP using the `hw-module slot stdby_slot_num reload` command and wait for the standby to reach Hot standby state.

**Step 7** Execute the `request platform software package install file rp active_slot_num file bootflash:asr903rsp1-sipspa.upgrade.pkg slot 0 bay im_slot_num force` command for each IM present in the router.

**Note** The IMs present are reset during the installation. Verify the IM state is OK before proceeding to the next IM.

**Step 8** Upgrade all the sub-packages on the active RSP using the `request platform software package install rp active_slot_num file bootflash:asr903rsp1-*.upgrade.pkg` command.

**Note** If you have missed the package installation on any of the IM in Step 7 and proceeded to Step 8, the packages are automatically installed for the missed IMs.

**Step 9** Perform a switchover. Wait for the new standby RSP module to reach hot standby state.

The latest image is upgraded on the router.
Upgrading the ROMMON on the RSP Module

The Cisco ASR 903 Router has two ROMMON regions (ROM0 and ROM1). We recommend that the upgrade is performed on both the regions.

⚠️ Caution
To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Follow the procedure to upgrade the ROMMON image:

### Step 1
Check the RSP bootup ROMMON region (ROM0 or ROM1). The example shows the RSP boots up from ROM0 region.

```
System Bootstrap, Version 15.2(1r)S1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Compiled Wed 07-Dec-11 07:33 by tinhuang
Current image running: Boot ROM0
```

### Step 2
Copy the ROMMON image to the bootflash on the active and standby RSP.

```
copy bootflash:asr903-rommon.153-1r.S1.pkg
```

### Step 3
Use the `upgrade rom-monitor filename bootflash:asr903-rommon.153-1r.S1.pkg R0` command to upgrade the version.

⚠️ Note
R0 represents RSP in slot0 of the chassis. **Step 3** upgrades the ROMMON region of the RSP that is not used (ROM1 region) as ROM 0 region is used (in this procedure) in **Step 1** to boot up the RSP.

### Step 4
Upgrade the ROMMON on the Standby RSP (for High Availability) using `upgrade rom-monitor filename bootflash:asr903-rommon.153-1r.S1.pkg R1` command.

⚠️ Note
R1 represents the RSP in slot1 of the chassis. **Step 4** upgrades the ROMMON region of the RSP that is not used (ROM 0 region).

### Step 5
Reload the router.

```
System Bootstrap, Version 15.2(1r)S1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Compiled Wed 07-Dec-11 07:33 by tinhuang
Current image running: Boot ROM0
```

```
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Rommon upgrade requested
Flash upgrade reset 1 in progress
......
```

```
System Bootstrap, Version 12.2(20120514:121217) [npenumar-pegasus_rommon_02 183], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2008 by cisco Systems, Inc.
Compiled Fri 15-Jun-12 11:45 by ccai
Current image running: *Upgrade in progress* Boot ROM1
```
Chapter 5 Installing and Upgrading Software

Software Upgrade Examples

Last reset cause: BootRomUpgrade
UEA platform with 2097152 Kbytes of main memory

Step 6

Reload the router again to confirm bootup from upgraded ROMMON region ROM1.

System Bootstrap, Version 15.2(1r)S1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Compiled Fri 15-Jun-12 11:45 by ccai
Current image running: Boot ROM1

Step 7

Repeat Step 3 to Step 6 to update the other region on the RSP (ROM0) region in this procedure.

Note

We recommend that both region ROM0 and ROM1 are upgraded.

Verifying the Upgrade

Use the show platform command to verify the ROMMON upgrade.

Router# show platform

Chassis type: ASR-903

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Insert time (ago)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0</td>
<td>A900-IMA1X</td>
<td>ok</td>
<td>04:48:07</td>
</tr>
<tr>
<td>0/1</td>
<td>A900-IMA1X</td>
<td>ok</td>
<td>04:43:42</td>
</tr>
<tr>
<td>0/4</td>
<td>A900-IMA8T</td>
<td>ok</td>
<td>05:18:21</td>
</tr>
<tr>
<td>0/5</td>
<td>A900-IMA8T</td>
<td>ok</td>
<td>05:18:21</td>
</tr>
<tr>
<td>R0</td>
<td>A903-RSP1A-55</td>
<td>ok, active</td>
<td>05:23:11</td>
</tr>
<tr>
<td>R1</td>
<td>A903-RSP1A-55</td>
<td>ok, standby</td>
<td>05:23:11</td>
</tr>
<tr>
<td>F0</td>
<td></td>
<td>ok, active</td>
<td>05:23:11</td>
</tr>
<tr>
<td>F1</td>
<td></td>
<td>ok, standby</td>
<td>05:23:11</td>
</tr>
<tr>
<td>P0</td>
<td>A900-PWR550-D</td>
<td>ok</td>
<td>05:20:02</td>
</tr>
<tr>
<td>P1</td>
<td>A900-PWR550-D</td>
<td>ok</td>
<td>05:19:55</td>
</tr>
<tr>
<td>P2</td>
<td>A903-FAN</td>
<td>ok</td>
<td>05:19:45</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot</th>
<th>CPLD Version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>R0</td>
<td>11102133</td>
<td>15.3(1r)S1</td>
</tr>
<tr>
<td>R1</td>
<td>11102133</td>
<td>15.3(1r)S1</td>
</tr>
<tr>
<td>F0</td>
<td>11102133</td>
<td>15.3(1r)S1</td>
</tr>
<tr>
<td>F1</td>
<td>11102133</td>
<td>15.3(1r)S1</td>
</tr>
</tbody>
</table>

Software Upgrade Examples

The following sections provide samples of software upgrades on the Cisco ASR 903 Series Router.

Single Command Software Upgrade

Router# request platform software package install node file bootflash:XE371_k9_0810.bin interface-module-delay 150
NOTE: Currently node has booted from a provisioning file
NOTE: Going to start a dual rp sub-packages node ISSU install

--- Starting initial file path checking ---
Copying bootflash:XE371_k9_0810.bin to stby-bootflash:XE371_k9_0810.bin
Finished initial file path checking

--- Starting config-register verification ---
Finished config-register verification

--- Starting image file expansion ---
Expanding image file: bootflash:XE371_k9_0810.bin
Image file expanded and copied
Expanding image file: stby-bootflash:XE371_k9_0810.bin
Image file expanded and copied
Finished image file expansion

STAGE 1: Installing software on standby RP
==========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax

    Found asr903rspi-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
    Found asr903rspi-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
    Found asr903rspi-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
    Found asr903rspi-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
    Found asr903rspi-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
    Found asr903rspi-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
    Found asr903rspi-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

Verifying image file sipspa
Inspecting image file types

    WARNING: In-service installation of IOSD package
--- Starting candidate package set construction ---

Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting compatibility testing ---

Determining whether candidate package set is compatible
Determining whether installation is valid
Determining whether installation is valid ... skipped
Verifying image type compatibility
Checking IPC compatibility for candidate software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Checking package specific compatibility
Finished compatibility testing

--- Starting list of software package changes ---
Old files list:
 Removed asr903rsp1-espbase.2012-08-12_15.26_amprajap.pkg
 Removed asr903rsp1-rpaccess.2012-08-12_15.26_amprajap.pkg
 Removed asr903rsp1-rpbase.2012-08-12_15.26_amprajap.pkg
 Removed asr903rsp1-rpcontrol.2012-08-12_15.26_amprajap.pkg
 Removed asr903rsp1-rpios-universalk9_npe.2012-08-12_15.26_amprajap.pkg
 Removed asr903rsp1-sipbase.2012-08-12_15.26_amprajap.pkg
 Removed asr903rsp1-sipspa.2012-08-12_15.26_amprajap.pkg

New files list:
 Added asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Added asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Added asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Added asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Added
 asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Added asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Added asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

SUCCESS: Software provisioned. New software will load on reboot.

STAGE 2: Restarting standby RP

STAGE 3: Installing sipspa package on local RP
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting compatibility testing ---
Determining whether candidate package set is compatible

WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

Determining whether installation is valid

WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

Software sets are identified as compatible
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished compatibility testing

--- Starting impact testing ---
Checking operational impact of change
Finished impact testing

--- Starting list of software package changes ---
Old files list:
  Removed asr903rsp1-sipspa.2012-08-12_15.26_amprajap.pkg
New files list:
Chapter 5  Installing and Upgrading Software

Software Upgrade Examples

Added asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
Finding latest command set
Finding latest command shortlist lookup file
Finding latest command shortlist file
Assembling CLI output libraries
Assembling CLI input libraries
Assembling Dynamic configuration files
Applying interim IPC and database definitions
Replacing running software
Replacing CLI software
Restarting software
Restarting IM: 0/0
Skipping IM reload for Ethernet IM
Restarting IM: 0/1
Skipping IM reload for Ethernet IM
Restarting IM: 0/2
Skipping IM reload for Ethernet IM
Restarting IM: 0/3
Skipping IM reload for Ethernet IM
Restarting IM: 0/4
Skipping IM reload for Ethernet IM
Applying final IPC and database definitions
Generating software version information
Notifying running software of updates
Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
Finished update running software
SUCCESS: Finished installing software.

STAGE 4: Installing software on active RP
=========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
Found asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Found asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Found asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Found asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Found
asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Found asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Found asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Verifying image file locations
Inspecting image file types
WARNING: In-service installation of IOSD package
WARNING: requires software redundancy on target RP
WARNING: or on-reboot parameter
WARNING: Automatically setting the on-reboot flag
WARNING: In-service installation of RP Base package
WARNING: requires software reboot of target RP
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting compatibility testing ---
Determining whether candidate package set is compatible
Determining whether installation is valid
Determining whether installation is valid ... skipped
Verifying image type compatibility
Checking IPC compatibility for candidate software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Checking package specific compatibility
Finished compatibility testing

--- Starting list of software package changes ---
Old files list:
  Removed asr903rsp1-espbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpaccess.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpcontrol.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpios-universalk9_npe.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-sipbase.2012-08-12_15.26_amprajap.pkg
New files list:
  Added asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned. New software will load on reboot.
STAGE 5: Restarting active RP (switchover to stdby)

--- Starting active reload ---

Finished active reload

SUCCESS: node ISSU finished successfully.

RUDY-1#

RUDY-1#Aug 24 07:54:41.715 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: reload fru action requested

System Bootstrap, Version 15.3(1r)S1, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2012 by cisco Systems, Inc.

Compiled Tue 26-Jun-12 12:42 by ccai

Current image running: Boot ROMUEA platform with 3670016 Kbytes of main memory

Located packages.conf
Image size 7519 inode num 38, bks cnt 2 blk size 8*512

Located asr903rp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Image size 34216240 inode num 90631, bks cnt 8354 blk size 8*512

Bootstrap image size = 34216240 (0x20a1930) bytes

Package header rev 0 structure detected

Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated e7674970:dbc1eb86:325219c7:b3da0e0f:077e5e4d
expected e7674970:dbc1eb86:325219c7:b3da0e0f:077e5e4d

Image validated

%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): load_crash_kernel took: 2 seconds, expected max time 2 seconds

%IOSXEBOOT-4-DEBUG_CONF: (rp/0): File /bootflash/debug.conf is absent, ignoring

%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): Chassis initialization took: 26 seconds, expected max time 10 seconds

%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): upgrade hw-programmable took: 2 seconds, expected max time 2 seconds

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version 15.2(20120810:081250) ([v152_4_s_xe37_throttle-BLD-BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021-ios 131])
Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Fri 10-Aug-12 03:50 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc. All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrq.html

If you require further assistance please contact us by sending email to export@cisco.com.

cisco ASR-903 (RSP1) processor with 540359K/6147K bytes of memory.
Processor board ID FOX1518P0GP
32768K bytes of non-volatile configuration memory.
3670016K bytes of physical memory.
1328927K bytes of SD flash at bootflash:

Press RETURN to get started!
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, page 6-1
- Configuring the Management Ethernet Port, page 6-1
- Configuring Console Ports, page 6-1
- Reloading the Route Switch Processor, page 6-1
- Forcing a Route Switch Processor Switchover, page 6-2

Configuring Timing Ports

For information about configuring timing ports on the RSP, see Chapter 11, “Configuring Clocking and Timing.”

Configuring the Management Ethernet Port

For information about configuring the management Ethernet port on the RSP, see Chapter 3, “Using the Management Ethernet Interface.”

Configuring Console Ports

For information about configuring console ports, see Chapter 2, “Console Port, Telnet, and SSH Handling.”

Reloading the Route Switch Processor

To reload the RSP, use the `hw-module slot reload` command in privileged EXEC mode.

`Router# hw-module slot r0 reload`
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.
CHAPTER 7

Configuring Ethernet Interfaces

This chapter provides information about configuring the Gigabit Ethernet interface modules on the Cisco ASR 900 Series Router. It includes the following sections:

- Configuring Ethernet Interfaces, page 7-1
- Verifying the Interface Configuration, page 7-9
- Verifying Interface Module Status, page 7-10
- Configuring LAN/WAN-PHY Controllers, page 7-11

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

### Configuring Ethernet Interfaces

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

This section includes the following topics:

- Limitations and Restrictions, page 7-1
- Configuring an Interface, page 7-2
- Specifying the Interface Address on an Interface Module, page 7-3
- Configuring Hot Standby Router Protocol, page 7-4
- Modifying the Interface MTU Size, page 7-5
- Configuring the Encapsulation Type, page 7-6
- Configuring Autonegotiation on an Interface, page 7-6
- Saving the Configuration, page 7-7
- Shutting Down and Restarting an Interface, page 7-8
- Configuring LAN-PHY Mode, page 7-12

### Limitations and Restrictions

Ten Gigabit Ethernet interface modules are not supported in slots 4 and 5.
Configuring an Interface

This section lists the required configuration steps to configure Gigabit and Ten Gigabit Ethernet interface modules. Follow these steps to configure your interface module:

SUMMARY STEPS

1. configure terminal
2. interface gigabitethernet slot/subslot/port
   or
   interface tengigabitethernet slot/subslot/port
3. ip address [ip-address mask {secondary} | dhcp {client-id interface-name} {hostname host-name}]
4. mtu bytes
5. standby [group-number] ip [ip-address {secondary}]
6. no shutdown

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>
| Step 2  | Router(config)# interface gigabitethernet slot/subslot/port  
   or  
   Router(config)# interface tengigabitethernet slot/subslot/port | Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where:  
   • slot/subslot/port—The location of the interface. See the “Specifying the Interface Address on an Interface Module” section on page 7-3.  
   Note  
   The slot number is always 0. |
| Step 3  | Router(config-if)# ip address [ip-address mask {secondary} | dhcp {client-id interface-name} {hostname host-name}] | Sets a primary or secondary IP address for an interface that is using IPv4, where:  
   • ip-address—The IP address for the interface.  
   • mask—The mask for the associated IP subnet.  
   • secondary—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.  
   • dhcp—Specifies that IP addresses will be assigned dynamically using DHCP.  
   • client-id interface-name—Specifies the client identifier. The interface-name sets the client identifier to the hexadecimal MAC address of the named interface.  
   • hostname host-name—Specifies the hostname for the DHCP purposes. The host-name is the name of the host to be placed in the DHCP option 12 field. |
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 Cisco ASR 900 Series Router where the interface module is installed.

  - **Note** The interface module slot number is always 0.

- **subslot**—The subslot where the interface module is installed. Interface module subslots are numbered from 0 to 5, 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:
Configuring Ethernet Interfaces

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 120.12.1.200
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
```

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:
    UpSerial10
    UpSerial11
```
Modifying the Interface MTU Size

Note

The maximum number of unique MTU values that can be configured on the physical interfaces on the Cisco ASR 900 Series router is 8. Use the show platform hardware pp active interface mtu command to check the number of values currently configured on the router.

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.
- Tag or Multiprotocol Label Switching (MPLS) MTU—Can be specified on an interface and allows up to six different tag headers to be attached to a packet. The maximum number of tag headers (also referred to as labels) depends on your Cisco IOS software release.

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 Cisco ASR 900 Series Router, 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
- If you are using MPLS, be sure that the mpls mtu command is configured for a value less than or equal to the interface MTU.
- 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 Configuration Task

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

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

### 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 1 (the second port) on the Gigabit Ethernet interface module installed in slot 1 of the Cisco ASR 900 Series Router:

```
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)
```

### 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 Cisco ASR 900 Series Router, flow control is autonegotiated when autonegotiation is enabled. Autonegotiation is enabled by default.

When enabling autonegotiation, consider these guidelines:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# 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>
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>Router(config-if)# negotiation auto</td>
<td>Enables autonegotiation on a Gigabit Ethernet interface. Advertisement of flow control occurs.</td>
</tr>
</tbody>
</table>

Disabling Autonegotiation

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

Speed and duplex configurations can be advertised using autonegotiation. However, the only values that are negotiated are:

- For Gigabit Ethernet interfaces using RJ-45 copper interfaces—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>Router(config-if)# no negotiation auto</td>
<td>Disables autonegotiation on Gigabit Ethernet interfaces. No advertisement of flow control occurs.</td>
</tr>
</tbody>
</table>

Configuring Carrier Ethernet Features

For information about configuring an Ethernet interface as a layer 2 Ethernet virtual circuit (EVC) or Ethernet flow point (EFP), see the Configuring Ethernet Virtual Connections on the Cisco ASR 900 Series Router document and the Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S.

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>Router# copy running-config startup-config</td>
<td>Writes the new configuration to NVRAM.</td>
</tr>
</tbody>
</table>
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.

There are no restrictions for online insertion and removal (OIR) of Gigabit Ethernet interface modules; you can remove them at any time.

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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# shutdown</td>
<td>Restarts, stops, or starts an interface.</td>
</tr>
</tbody>
</table>

You can use the following commands 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>Router# hw-module slot number (logging ) reload [force]</td>
<td>Restarts, stops, or starts a slot on the router. You can also use this command to disable or enable onboard logging of the hardware.</td>
</tr>
<tr>
<td>start</td>
<td>stop [force]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# hw-module subslot slot/subslot reload [force]</td>
<td>Restarts, stops, or starts a subslot and its interfaces. You can also use this command to disable or enable onboard logging of the hardware.</td>
</tr>
<tr>
<td>start</td>
<td>stop [force]</td>
</tr>
</tbody>
</table>

In similar fashion, you do not need to independently restart any interfaces on an interface module after OIR.

To shut down an interface on an interface module, 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)# shutdown</td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>

To enable traffic on an interface, use the following command in interface configuration mode:
Verifying the Interface Configuration

Besides using the `show running-configuration` command to display your Cisco ASR 900 Series Router 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 of the Cisco ASR 900 Series Router:

```
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: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: fifo
   Output queue: 0/40 (size/max)
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
   11 packets input, 704 bytes, 0 no buffer
   Received 11 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   0 packets output, 0 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```
Verifying Interface Module Status

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

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

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

The following `show hw-module subslot` command sample output is for CWDM 1490:

```
Router# `show hw-module subslot 2/0 transceiver 2 idprom`
IDPROM for transceiver GigabitEthernet2/0/2:
Description = SFP optics (type 3)
Transceiver Type: = GE CWDM 1490 (28)
Product Indentifier (PID) = FWDM-16217D49CSC
Vendor Revision = C
Serial Number (SN) = FNS10500HA9
Vendor Name = CISCO-FINISAR
Vendor OUI (IEEE company ID) = 00.90.65 (36965)
CLEI code = CNTRVX0FAA
Cisco part number = 10-1884-01
Device State = Enabled.
Date code (yy/mm/dd) = 06/12/12
Connector type = LC.
Encoding = 8B10B
NRZ
Nominal bitrate = (2700 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
```

The following `show hw-module subslot` command sample output is for an XFP module:

```
Router# `show hw-module subslot 2/2 transceiver 0 idprom brief`
IDPROM for transceiver TenGigabitEthernet2/2/0:
Description = XFP optics (type 6)
Transceiver Type: = OC192 + 10GBASE-L (97)
Product Indentifier (PID) = TRF5011AN-LF004
Vendor Revision = 05
Serial Number (SN) = ONT11061053
Vendor Name = CISCO-OPNEXT
Vendor OUI (IEEE company ID) = 00.0B.40 (2880)
CLEI code = WMOTBEVAAB
Cisco part number = 10-1989-02
```
Device State = Enabled.
Date code (yy/mm/dd) = 07/02/06
Connector type = LC.
Encoding = 64B/66B
SONET Scrambled
NRZ
Minimum bit rate = 9900 Mbits/s
Maximum bit rate = 10500 Mbits/s

The following show hw-module subslot command sample output is for an XFP module:

Router# show hw-module subslot 0/3 transceiver 0 status
The Transceiver in slot 0 subslot 3 port 0 is enabled.
Module temperature = 38.183 C
Transceiver Tx bias current = 37968 uAmps
Transceiver Tx power = -2.3 dBm
Transceiver Rx optical power = -0.7 dBm

Configuring LAN/WAN-PHY Controllers

The LAN/WAN-PHY controllers are configured in the physical layer control element of the Cisco IOS XE software. Use the hw-module subslot slot/subslot enable lan command to configure the LAN-PHY mode.

Configuration of the LAN/WAN-PHY controllers is described in the following tasks.

- Configuring LAN-PHY Mode, page 7-12
- Configuring WAN-PHY Signal Failure and Signal Degrade Bit Error Rates, page 7-13
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 interface-path-id`
2. `configure terminal`
3. `hw-module subslot subslot/port enable LAN`
4. `exit`
5. `show controllers wanphy slot/subslot/port`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `show controllers wanphy 0/1/0`<br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br>
Chapter 7  Configuring Ethernet Interfaces

Configuring LAN/WAN-PHY Controllers

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 declared 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 of link quality degradation is triggered. The WAN-PHY alarms are required for some users who are upgrading their Layer 2 core network from a SONET ring to a 10-Gigabit Ethernet ring.

Prerequisites

This section describes the prerequisites for configuring the BER threshold values on an Ethernet interface module:

Note

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>hw-module subslot slot/subslot enable LAN Configures the LAN PHY mode for the Ethernet interface module.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# hw-module subslot 0/1 enable LAN</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit Exits global-configuration (config) mode and enters privilege-exec mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# exit</td>
</tr>
<tr>
<td>Step 5</td>
<td>show controllers wanphy 0/1/0 Displays the configuration mode for the LAN/WAN-PHY controller. The example shows the mode of operation as LAN mode for the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show controllers wanphy 0/1/0 TenGigabitEthernet0/1/0 Mode of Operation: LAN Mode</td>
</tr>
</tbody>
</table>

Configuring WAN-PHY Signal Failure and Signal Degrade Bit Error Rates

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 declared 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 of link quality degradation is triggered. The WAN-PHY alarms are required for some users who are upgrading their Layer 2 core network from a SONET ring to a 10-Gigabit Ethernet ring.

Prerequisites

This section describes the prerequisites for configuring the BER threshold values on an Ethernet interface module:

Note

The controller must be in the WAN-PHY mode prior to configuring the SF and SD BER reporting and thresholds.
Configuration Examples

This section includes the following configuration examples:

- Example: Basic Interface Configuration, page 7-14
- Example: MTU Configuration, page 7-14
- Example: VLAN Encapsulation, page 7-15

Example: Basic Interface Configuration

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

! Enter global configuration mode.

Router# configure terminal

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

! Specify the interface address.

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

! Configure an IP address.

Router(config-if)# ip address 192.168.50.1 255.255.255.0

! Start the interface.

Router(config-if)# no shut

! Save the configuration to NVRAM.

Router(config-if)# exit

Router# copy running-config startup-config

Example: MTU Configuration

Note: The maximum number of unique MTU values that can be configured on the physical interfaces on the Cisco ASR 900 Series router is 8. Use the show platform hardware pp active interface mtu command to check the number of values currently configured on the router.

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

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

! Enter global configuration mode.

! Router# configure terminal
Configuration Examples

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.
! ! Specify the interface address
! Router(config)# service instance 10 ethernet
! ! Configure dot1q encapsulation and specify the VLAN ID.
! Router(config-subif)# encapsulation dot1q 268

VLANs are only supported on EVC service instances and Trunk EFP interfaces. For more information about how to configure these features, see the Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S.
Configuring T1/E1 Interfaces

This chapter provides information about configuring the T1/E1 interface module on the Cisco ASR 900 Series Router. It includes the following sections:

- Configuration Tasks, page 8-1
- Verifying the Interface Configuration, page 8-14
- Configuration Examples, page 8-15

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

This section describes how to configure the T1/E1 interface module for the Cisco ASR 900 Series Router and includes the following topics:

- Limitations, page 8-1
- Required Configuration Tasks, page 8-2
- Optional Configurations, page 8-4
- Saving the Configuration, page 8-10

Limitations

This section describes the software limitations that apply when configuring the T1/E1 interface module on the Cisco ASR 900 Series Router.

- The Cisco ASR 900 Series Router does not support more than 16 IMA groups on each T1/E1 interface module.
- The Cisco ASR 900 Series Router only supports the following BERT patterns: $2^{11}$, $2^{15}$, $2^{20}$-$O153$, and $2^{20}$-$QRSS$.
- L2TPv3 encapsulation is not supported on the Cisco ASR 900 Series router.
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, page 8-2
- Configuring the Controller, page 8-3
- Verifying Controller Configuration, page 8-4
- Optional Configurations, page 8-4

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 Router(config)# card type {e1</td>
<td>Sets the serial mode for the interface module:</td>
</tr>
<tr>
<td>t1} slot subslot</td>
<td></td>
</tr>
<tr>
<td>- t1—Specifies T1 connectivity of 1.536 Mbps. B8ZS is the default</td>
<td></td>
</tr>
<tr>
<td>- e1—Specifies a wide-area digital transmission scheme used</td>
<td></td>
</tr>
<tr>
<td>- slot subslot—Specifies the location of the interface module.</td>
<td></td>
</tr>
<tr>
<td>Step 3 Router(config)# exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter</td>
</tr>
<tr>
<td></td>
<td>prompt.</td>
</tr>
</tbody>
</table>
## Configuring the Controller

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router# <code>configure terminal</code>&lt;br&gt;Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config)# `controller {t1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-controller)# `clock source {internal</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config-controller)# `linecode {ami</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>For T1 Controllers:</strong>&lt;br&gt;Router(config-controller)# `framing {sf</td>
</tr>
</tbody>
</table>
Configuration Tasks

Chapter 8 Configuring T1/E1 Interfaces

Verifying Controller Configuration

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

```
Router# show controllers t1 0/3/0 brief
T1 0/3/0 is up.
Applique type is A900-IMA16D
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
    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)
    136 Line Code Violations, 63 Path Code Violations,
    0 Slip Secs, 6 Fr Loss Secs, 4 Line Err Secs, 0 Degraded Mins,
    7Errored 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, page 8-5
- Setting an IP Address, page 8-6
- Configuring Encapsulation, page 8-6
- Configuring the CRC Size for T1 Interfaces, page 8-8
- Configuring a Channel Group, page 8-9
- Saving the Configuration, page 8-10
## 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.

### Command Purpose

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# controller {t1</td>
<td>e1} {slot/subslot/port}</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# controller {t1</td>
<td>e1} {slot/subslot/port}</td>
</tr>
<tr>
<td>Step 3</td>
<td>For T1 controllers</td>
<td>Sets the framing on the interface.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-controller)# framing {sf</td>
<td>esf}</td>
</tr>
<tr>
<td>Step 3</td>
<td>For E1 controllers</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-controller)# framing {crc4</td>
<td>no-crc4}</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
</tbody>
</table>

### Configuring Framing

#### Configuration Tasks

#### Step 1

Enter global configuration mode.

#### Step 2

Selects the controller to configure.

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

#### Note

The slot number is always 0.

#### Step 3

For T1 controllers

- Router(config-controller)# framing \{sf \| esf\}

For E1 controllers

- Router(config-controller)# framing \{crc4 \| no-crc4\}

#### Step 4

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

### Verifying Framing Configuration

Use the **show controllers** command to verify the framing configuration:

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Router(config)# interface serial 0/subslot/port:channel-group</strong></td>
</tr>
<tr>
<td></td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>subslot</strong>—Specifies the subslot in which the T1/E1 interface module is installed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>port</strong>—Specifies the location of the controller. The port range for T1 and E1 is 1 to 16.</td>
</tr>
<tr>
<td></td>
<td>• <strong>channel-group</strong>—Specifies the channel group number configured on the controller. For example: interface serial 0/0/1:1.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Router(config-if)# ip address address mask</strong></td>
</tr>
<tr>
<td></td>
<td>Sets the IP address and subnet mask.</td>
</tr>
<tr>
<td></td>
<td>• <strong>address</strong>—Specify the IP address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>mask</strong>—Specify the subnet mask.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Router(config)# exit</strong></td>
</tr>
<tr>
<td></td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
</tbody>
</table>

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 on the Cisco ASR 900 Series router.
To set the encapsulation method, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# interface serial 0/subslot/port:channel-group</td>
</tr>
<tr>
<td></td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>- subslot— Specifies the subslot in which the T1/E1 interface module is installed.</td>
</tr>
<tr>
<td></td>
<td>- port— Specifies the location of the controller. The port range for T1 and E1 is 1 to 16.</td>
</tr>
<tr>
<td></td>
<td>- channel-group— Specifies the channel group number configured on the controller. For example: interface serial 0/0/1:1.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-if)# encapsulation encapsulation-type {hdlc</td>
</tr>
<tr>
<td></td>
<td>Set the encapsulation method on the interface.</td>
</tr>
<tr>
<td></td>
<td>- hdlc— High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces.</td>
</tr>
<tr>
<td></td>
<td>- ppp— Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config)# exit</td>
</tr>
<tr>
<td></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:

```
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
5 packets input, 0 bytes, 0 no buffer
81 packets output, 0 bytes, 0 underruns
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
64 packets output, 0 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# interface serial 0/number:channel-group</td>
</tr>
<tr>
<td></td>
<td>• number—Specifies the location of the controller. The number range for T1 and E1 is 1 to 16.</td>
</tr>
<tr>
<td></td>
<td>• channel-group—Specifies the channel group number configured on the controller. For example: interface serial 0/1:1.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-if)# crc {16</td>
</tr>
<tr>
<td></td>
<td>• 16—16-bit CRC. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• 32—32-bit CRC.</td>
</tr>
<tr>
<td></td>
<td>Note Moving from CRC 16 to 32 bit (and vice-versa) is not supported.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>

Verifying the CRC Size

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

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

Follow these steps to configure a channel group:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller {t1</td>
<td>e1}</td>
</tr>
<tr>
<td>slot/subslot/port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# channel-group {t1</td>
<td>e1} number {timeslots range</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• unframed—Unframed mode (G.703) uses all 32 time slots for data. None of the 32 time slots are used for framing signals.</td>
</tr>
<tr>
<td></td>
<td>• speed—(Optional) Specifies the speed of the underlying DS0s in kilobits per second. Valid values are 56 and 64.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The default is 64. Speed is not mentioned in the configuration.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Each channel group is presented to the system as a serial interface that can be configured individually.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Once a channel group has been created with the channel-group command, the channel group cannot be changed without removing the channel group. To remove a channel group, use the no form of the channel-group command.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The unframed option is not currently supported.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>DS0-level channelization is not currently supported.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Exit configuration mode when you have finished configuring the controller.</td>
<td>end</td>
</tr>
</tbody>
</table>
## 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>Router# <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
- Running Bit Error Rate Testing

### Setting Loopbacks

The following sections describe how to set loopbacks:

- Setting a Loopback on the E1 Controller, page 8-10
- Setting a Loopback on the T1 Controller, page 8-11

### 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>Router# <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Select the E1 controller and enter controller configuration mode.</td>
<td><code>controller e1 slot/subslot/port</code></td>
</tr>
<tr>
<td>Note</td>
<td>The slot number is always 0.</td>
</tr>
<tr>
<td>Set a diagnostic loopback on the E1 line.</td>
<td><code>loopback diag</code></td>
</tr>
<tr>
<td>Set a network payload loopback on the E1 line.</td>
<td>`loopback network [line</td>
</tr>
<tr>
<td>Exit configuration mode when you have finished configuring the controller.</td>
<td><code>end</code></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>Selects the T1 controller and enter controller configuration mode.</td>
<td><code>controller t1 slot/subslot/port</code></td>
</tr>
<tr>
<td>Sets a diagnostic loopback on the T1 line.</td>
<td><code>loopback diag</code></td>
</tr>
<tr>
<td>Sets a local loopback on the T1 line. You can select to loopback the line or the payload.</td>
<td>`loopback local {line</td>
</tr>
<tr>
<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>
<td><code>loopback remote iboc</code></td>
</tr>
<tr>
<td>Exits configuration mode when you have finished configuring the controller.</td>
<td><code>end</code></td>
</tr>
</tbody>
</table>

**Note**

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

**Table 8-1 Loopback Descriptions**

<table>
<thead>
<tr>
<th>Loopback</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>loopback diag</code></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 <code>clock source</code> command to <code>internal</code> for this loopback mode.</td>
</tr>
<tr>
<td><code>loopback local</code></td>
<td>Loops the incoming receive signal back out to the transmitter. You can specify whether to use the <code>line</code> or <code>payload</code>.</td>
</tr>
<tr>
<td><code>local line</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>local payload</code></td>
<td>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 <code>clock source</code> command). When the payload loopback is ended, the clock source returns to the last setting selected by the <code>clock source</code> command.</td>
</tr>
</tbody>
</table>
### Configuration Tasks

#### Runing Bit Error Rate Testing

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

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

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

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

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selects the E1 or T1 controller and enters controller configuration mode.</td>
<td>`Router(config)# controller {e1</td>
</tr>
<tr>
<td>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.</td>
<td>`Router(config-controller)# bert pattern {0s</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Table 8-2</th>
<th><strong>BERT Pattern Descriptions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keyword</strong></td>
<td><strong>Description</strong></td>
</tr>
<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 O.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.

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

You can view the results of a BERT test at the following times:
- After you terminate the test using the **no bert** command
- After the test runs completely
- Anytime during the test (in real time)
Verifying the Interface Configuration

Besides using the `show running-configuration` command to display your Cisco ASR 900 Series Router configuration settings, you can use the `show interfaces serial` and the `show controllers serial` commands to get detailed information on a per-port basis for your T1/E1 interface module.

Verifying Per-Port Interface Status

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

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

**Configuration Examples**

This section includes the following configuration examples:

- Example: Framing and Encapsulation Configuration, page 8-15
- Example: CRC Configuration, page 8-15
- Example: Facility Data Link Configuration, page 8-16
- Example: Invert Data on the T1/E1 Interface, page 8-16

**Example: Framing and Encapsulation Configuration**

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

```plaintext
! 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:

```plaintext
! 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
```
Example: Facility Data Link Configuration

The following example configures Facility Data Link:

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

Example: Invert Data on the T1/E1 Interface

The following example inverts the data on the serial interface:

! Enter global configuration mode
! Router# configure terminal
! Specify the serial interface and enter interface configuration mode
! Router(config)# interface serial 2/1/3:0
! Configure invert data
! Router(config-if)# invert data
! Exit interface configuration mode and return to global configuration mode
! Router(config-if)# exit
! Exit global configuration mode
! Router(config)# exit
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 9-1 contains the wavelength mapping information for the DWDM-XFP-C module.

<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>192.0</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>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>
</tbody>
</table>
### Table 9-1 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>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>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>
</tbody>
</table>
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`

---

**Table 9-1: 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>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>
<tr>
<td>69</td>
<td>1534.61</td>
<td>195.35</td>
</tr>
<tr>
<td>70</td>
<td>1534.29</td>
<td>195.4</td>
</tr>
<tr>
<td>71</td>
<td>1533.82</td>
<td>195.45</td>
</tr>
<tr>
<td>72</td>
<td>1533.5</td>
<td>195.5</td>
</tr>
<tr>
<td>73</td>
<td>1533.04</td>
<td>195.55</td>
</tr>
<tr>
<td>74</td>
<td>1532.72</td>
<td>195.6</td>
</tr>
<tr>
<td>75</td>
<td>1532.26</td>
<td>195.65</td>
</tr>
<tr>
<td>76</td>
<td>1531.94</td>
<td>195.7</td>
</tr>
<tr>
<td>77</td>
<td>1531.48</td>
<td>195.75</td>
</tr>
<tr>
<td>78</td>
<td>1531.14</td>
<td>195.8</td>
</tr>
<tr>
<td>79</td>
<td>1530.69</td>
<td>195.85</td>
</tr>
<tr>
<td>80</td>
<td>1530.37</td>
<td>195.9</td>
</tr>
<tr>
<td>81</td>
<td>1529.91</td>
<td>195.95</td>
</tr>
<tr>
<td>82</td>
<td>1529.59</td>
<td>196</td>
</tr>
</tbody>
</table>
**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 the privileged EXEC mode. If prompted, enter your password.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters the global configuration mode.</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> interface tengigabitethernet slot/port</td>
<td>Specifies the 10-Gigabit Ethernet interface to be configured.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface tengigabitethernet 0/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> itu channel number</td>
<td>Sets the ITU channel.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# itu channel 28</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the ITU Configuration

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

```sh
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:** = IP9IAGGCCAB

**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 00 00 00 9E 20 00 00 00 00
070: 00 00 00 00 00 00 00 00 1B 7C 00 00
080: 00 00 00 00 00 00 00 00 00 00 00 00
090: 00 00 00 00 00 00 00 00 00 00 01 00
100: 00 00 00 00 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 00 00 00 01 00

**<<See byte 113, the hexa decimal equivalent for ITU channel 20>>**
XFP IDPROM Page 0x1:
128: 0C 98 07 00 00 00 00 00 00 00
138: 08 B4 63 71 50 00 00 00 00 9F
148: 43 49 53 43 4F 2D 4A 44 53
Configuring Optical Interface Modules

This chapter describes the most common configurations for optical interface modules on the Cisco ASR 900 Series Router and includes the following sections:

- Limitations and Restrictions, page 10-1
- Configuring the Controller, page 10-2
- Configuring SDH, page 10-2
- Configuring SONET Mode, page 10-6
- Configuring a CEM group, page 10-9
- Configuring DS3 Clear Channel on OC-3 and OC-12 Interface Module, page 10-13
- Optional Configurations, page 10-16
- Managing Interface Naming, page 10-19
- Configuring Multilink Point-to-Point Protocol, page 10-20
- Configuring BERT, page 10-22
- Configuring Automatic Protection Switching, page 10-22
- Configuring Automatic Protection Switching, page 10-22
- Configuring Automatic Protection Switching, page 10-22
- Verifying Interface Configuration, page 10-23
- Troubleshooting, page 10-23
- Configuration Examples, page 10-24
- Additional Resources, page 10-25

Limitations and Restrictions

The following limitations and restrictions apply when configuring optical interface modules on the Cisco ASR 900 Series Router:

- SDH framing mode is supported; SONET framing is supported beginning in Release 3.8.
- HDLC, PPP, and MLPPP encapsulation are supported. In POS mode, HDLC and PPP are supported.
- Frame Relay and SMDS encapsulation are not supported.
- ATM Layer 2 AAL0 and AAL5 encapsulation types are supported.
Configuring the Controller

Use the following command to configure the controller for SONET or SDH framing:

```
Router(config)# controller sonet slot/subslot/port
```

**Note**

When the mode is changed, the interface module reloads.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Router(config)# controller sonet slot/subslot/port | Selects the controller to configure and enters controller configuration mode, where:  
  - `slot/subslot/port`—Specifies the location of the interface.  
  **Note** The slot number is always zero on the Cisco ASR 900 Series Router. |

Configuring SDH

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

- Configuring SDH Mode, page 10-3
- Configuring SDH in POS Mode, page 10-5
## Configuring SDH Mode

To configure SDH mode, complete the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router(config-controller)# <strong>framing</strong> sdh</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config-controller)# <strong>aug</strong> mapping {au-3</td>
</tr>
<tr>
<td></td>
<td>If the AUG mapping is configured to be AU-4, then the following muxing, alignment, and mapping will be used: TUG-3 &lt;-- VC-4 &lt;-- AU-4 &lt;-- AUG</td>
</tr>
<tr>
<td></td>
<td>If the mapping is configured to be AU-3, then the following muxing, alignment, and mapping will be used: VC-3 &lt;-- AU-3 &lt;-- AUG</td>
</tr>
<tr>
<td></td>
<td>The default setting is <strong>au-3</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-controller)# <strong>clock</strong> source {internal</td>
</tr>
<tr>
<td></td>
<td>• <strong>internal</strong>—Specifies that the internal clock source is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>line</strong>—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>Router(config-controller)# <strong>au-4</strong> au-4# tug-3 tug-3#</td>
</tr>
<tr>
<td></td>
<td>Depending on the framing mode of SONET or SDH, each STS-1, AU-3, TUG-3, and AU-4 can be configured with one of these commands.</td>
</tr>
<tr>
<td></td>
<td>Depending on currently configured AUG mapping setting, this command further specifies TUG-3, AU-3, AU-4 or STS-1 muxing. The CLI command parser enters into config-ctrlr-tug3 (SDH mode), config-ctrlr-au3 (SDH mode), or config-ctrlr-sts1 parser mode (SONET mode), which makes only relevant commands visible.</td>
</tr>
<tr>
<td></td>
<td>• <strong>au-4#</strong>—Range is from 1 to 4 for OC-12 mode and 1 for OC-3 mode</td>
</tr>
<tr>
<td></td>
<td>• <strong>tug-3#</strong>—Range is from 1 to 3.</td>
</tr>
<tr>
<td></td>
<td>• <strong>au-3#</strong> —Range is from 1 to 12 for OC-12 mode. For OC-3 mode, the value is 1–3.</td>
</tr>
</tbody>
</table>
## Configuring SDH

### Example
```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# fraking 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)# mode e3
Router(config-controller-tug3)# tug-2 1 e1 1 cem-group 1 unframed
```

### Step 5
In SDH framing in AU-4 mode:
```
Router(config-controller-tug3)# mode (c-11 | c-12 | t3 | e3)
```
In SDH framing AU-3 mode:
```
Router(config-controller-au3)# mode (c-11 | c-12 | t3 | e3)
```

Configures mode of operation for AU-3 or AU-4 mode, where:
- **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.
- **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.
- **t3**—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) T3.
- **e3**—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) E3.

**Note**
Only c-11 and c-12 are currently supported.

### Step 6
**SAToP CEM Group**
```
Router(config-controller-tug3)# tug-2 1 e1 1 cem-group 1 unframed
```

**CESoPSN CEM Group**
```
Router(config-controller-tug3)# tug-2 1 e1 1 cem-group 1 timeslots 1-31
```

**Clear-Channel ATM**
```
Router(config-controller-tug3)# tug-2 1 e1 1 atm
```

**IMA Group**
```
Router(config-controller-tug3)# tug-2 1 e1 1 ima-group 1
```

**Channel Group**
```
Router(config-controller-tug3)# tug-2 1 e1 1 [channel-group channel-group-number] [timeslots list-of-timeslots]
```

Creates a CEM group, IMA group, or channel-group for the AU-3 or AU-4. Valid values are:
- **e1**—1–3
- **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.
### 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/interface-id`
2. `framing sdh`
3. `aug mapping au-4`
4. `au-4 au4-number pos`
5. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router(config)# <code>controller sonet 0/1/0</code></td>
</tr>
<tr>
<td></td>
<td>Selects the controller to be configured.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`framing {sonet</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# <code>framing sdh</code></td>
</tr>
<tr>
<td></td>
<td>Specifies SDH as the framing mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The interface module reloads if the framing is changed.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`aug mapping {au-3</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-controller)# <code>aug mapping au-4</code></td>
</tr>
<tr>
<td></td>
<td>Specifies AUG mapping.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> POS mode is only supported with AU-4 mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>au-4 au4-number pos</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-controller)# <code>au-4 1 pos</code></td>
</tr>
<tr>
<td></td>
<td>Selects the AU-4 to be configured in POS mode with SDH framing. The command creates a POS interface, such as POS0/0/1:1. In OC-3 mode, the value is 1; in OC-12 mode, valid values are 1-4.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-controller)# <code>end</code></td>
</tr>
<tr>
<td></td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>
Configuring SONET Mode

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

- Configuring SONET Mode, page 10-6
- Configuring SONET POS Mode, page 10-8

Configuring SONET Mode

To configure an interface module to use SONET mode:

**SUMMARY STEPS**

1. **framing sonet**
2. **clock source {line | internal}**
3. **sts-1 starting-number - ending-number**
4. **mode**
5. **vtg vtg_number t1 t1_line_number cem-group channel-number 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> <strong>controller sonet slot/subslot/port</strong></td>
<td>Selects the controller to be configured.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller sonet 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 1</strong> **framing {sonet</td>
<td>sdh}**</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# framing sonet</td>
<td></td>
</tr>
</tbody>
</table>
Step 2

**clock source {line | internal}**

**Example:**
```
Router(config-if)# clock source line
```

**Purpose:** Specifies the clock source for the POS link, where:
- **line**—The link uses the recovered clock from the line. This is the default setting.
- **internal**—The link uses the internal clock source.

Step 3

**sts-1 {1 - 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12}**

**Example:**
```
Router(config-controller)# sts-1 1 - 3
```

**Purpose:** 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.

**Note** The 1-12 value is supported only in OC-12 mode.

Step 4

**mode {t3 | vt-15}**

**Example:**
```
Router(config-ctrlr-sts1)# mode t3
```

**Purpose:** Specifies the mode of operation of an STS-1 path, where:

**Note** VT-15 is the only supported mode.
- **t3**—STS-1 carries an unchannelized (clear channel) T3.
- **vt-15**—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.

Step 5

**vtg vtg_number t1 t1_line_number cem-group channel-number timeslots list-of-timeslots**

**Example:**
```
Router(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 1 timeslots 1-10
```

**Purpose:** Configures the T1 on the VTG, where:
- **vtg**—Specifies the VTG number. For SONET framing, values are 1 to 7.

Step 6

**end**

**Example:**
```
Router(config-if)# end
```

**Purpose:** Exits configuration mode.

**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)# sts-1 1 - 3
Router(config-ctrlr-sts1)# mode t3
Router(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 1 timeslots 1-10
Router(config-controller)# end
```

For information on optional SONET configurations, see “Optional Configurations” section on page 16.
For information on optional ATM, IMA, POS and Serial interface configuration, see “Optional Configurations” section on page 16.
Configuring SONET 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`
3. `clock source {line | internal}`
4. `sts-1 starting-number - ending-number pos`
5. `exit`
6. `interface pos slot/subslot/port:sts-1#`
7. `encapsulation encapsulation-type`
8. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>controller sonet slot/subslot/port</code></td>
<td>Selects the controller to be configured.</td>
</tr>
<tr>
<td>Example: <code>Router(config)# controller sonet 0/1/0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> `framing {sonet</td>
<td>sdh}`</td>
</tr>
<tr>
<td>Example: <code>Router(config-controller)# framing sonet</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `clock source {line</td>
<td>internal}`</td>
</tr>
<tr>
<td>Example: <code>Router(config-controller)# clock source line</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `sts-1 {1-12</td>
<td>1-3</td>
</tr>
<tr>
<td>Example: <code>Router(config-controller)# sts-1 1 - 3 pos</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>exit</code></td>
<td>Exits controller configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Router(config-controller# exit</code></td>
<td></td>
</tr>
</tbody>
</table>
**Configuring a CEM group**

- Configuring CEM Group in SONET Mode, page 10-9
- Configuring CEM Group in SDH Mode, page 10-11

**Configuring CEM Group in SONET Mode**

To configure a T1 CEM group in SONET mode:

```
Router(config-if)# interface POS0/0/1
Router(config-if)# encapsulation hdlc
```

For information on optional SONET configurations, see “Configuring SONET POS Mode” section on page 8.
## 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.  
  |                  | - Enter your password if prompted |
| 2    | configure terminal | Enters global configuration mode. |
| 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.  
  | Example:         | Note: The slot number is always 1 and the bay number is always 0. |
| 4    | framing {sonet | sonet} | Specifies SONET as the framing mode.  
  |                  | Example:  
  |                  | Router(config)# framing sonet |
| 5    | 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.  
  | Example:         | 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.  
  |                  | Note: The 1-12 value is supported only in OC-12 mode. |
| 6    | mode { t3 | vt-15} | Specifies the mode of operation of an STS-1 path, where:  
  | Example:         | Note: VT-15 is the only supported mode.  
  |                  | - t3—DS3 clear channel mode. STS-1 carries an unchannelized (clear channel) T3.  
  |                  | - vt-15—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. |
| 7    | vtg vtg_number t1 t1_line_number cem-group channel-number timeslots list-of-timeslots | Configures the T1 on the VTG, where:  
  | Example:         | - vtg_number—Specifies the VTG number. For SONET framing, values are 1 to 7.  
  |                  | - t1_line_number—Specifies the T1 line number. Valid range is 1 to 4.  
  |                  | - channel-number—Specifies the channel number. Valid range is 0 to 2015.  
  |                  | - list-of-timeslots—Specifies the list of timeslots. Valid range is from 1 to 24. |
| 8    | end              | Exits controller configuration mode and returns to privileged EXEC mode. |
**Configuring CEM Group in SDH Mode**

To configure CEM group in SDH mode:

<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><strong>Note</strong>  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>
</tbody>
</table>
|      |                   | **Example:**  
|      |                   | Router(config)# controller sonet 0/1/0 |
|      |                   | **Example:**  
|      |                   | Router(config)# framing sdh |
Configuring a CEM group

Example

```
Router(config-controller)# au-4 3
```

**Step 5**

**au-4 au-4# tug-3 tug-3#**

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

In SDH framing mode, each 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.

  **Note** DS3 configuration is supported only on AuU-4.

- **tug-3#**—Range is from 1 to 3.

  **Note** T1 can only be configured in au-3 mode, E1 can only be configured in the au-4 mode.

Example:

```
Router(config-controller)# au-4 3
```

**Step 6**

```mode {t3 | 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.

Example:

```
Router(config-ctrlr-au3)# mode e3
```

**Step 7**

```cem-group group-number {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.

Example:

```
Router(config-ctrlr-au3)# cem-group 4 unframed
```

**Step 8**

```end```

Exits controller configuration mode and returns to privileged EXEC mode.

Example:

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# au-4 3
Router(config-ctrlr-au3)# mode e3
Router(config-ctrlr-au3)# cem-group 4 unframed
Router(config-ctrlr-au3)# end
```
Configuring DS3 Clear Channel on OC-3 and OC-12 Interface Module

- Configuring DS3 Clear Channel in SONET Mode, page 10-13
- Configuring DS3 Clear Channel in SDH Mode, page 10-14

Configuring DS3 Clear Channel in SONET Mode

To configure DS3 clear channel in SONET mode:

**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.  
  • Enter your password if prompted |
| 2    | configure terminal | Enters global configuration mode. |
| 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.  
  **Note**  
The slot number is always 1 and the bay number is always 0.  
  Example:  
  Router(config)# controller sonet 0/4/1 |
| 4    | framing {sonet | sdh} | Specifies SONET as the framing mode.  
  Example:  
  Router(config)# framing sonet |
| 5    | clock source {line | internal} | Specifies the clock source for the POS link, where:  
  • line—The link uses the recovered clock from the line. This is the default setting.  
  • internal—The link uses the internal clock source.  
  Example:  
  Router(config-if)# clock source internal |
| 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 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.  
  Example:  
  Router(config-controller)# sts-1 1 |
Configuring DS3 Clear Channel in SDH Mode

To configure DS3 clear channel in SDH mode:

**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>Example: Router(config)# controller sonet 0/1/0</td>
<td>slot/bay/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The slot number is always 1 and the bay number is always 0.</td>
</tr>
<tr>
<td><strong>Step 4</strong> framing</td>
<td>Specifies SDH as the framing mode.</td>
</tr>
<tr>
<td>Example: Router(config-controller)# framing sdh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> clock source</td>
<td>Specifies the clock source for the POS link, where:</td>
</tr>
<tr>
<td>Example: Router(config-controller)# clock source line</td>
<td>line—The link uses the recovered clock from the line. This is the default setting.</td>
</tr>
<tr>
<td><strong>Step 6</strong> aug mapping au-4</td>
<td>Configures AUG mapping for SDH framing.</td>
</tr>
<tr>
<td>Example: Router(config-controller)# aug mapping au-4</td>
<td>If the AUG mapping is configured to be AU-4, then the following muxing, alignment, and mapping will be used:</td>
</tr>
<tr>
<td></td>
<td>TUG-3 &lt;-- VC-4 &lt;-- AU-4 &lt;-- AUG.</td>
</tr>
</tbody>
</table>
## Configuring DS3 Clear Channel on OC-3 and OC-12 Interface Module

### Step 7
**Example**
```
Router(config-controller)# au-4 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.

### Step 8
**Example**
```
Router(config-ctrlr-au4)# mode e3
```
Specifies the mode of operation.

- `e3`—Specifies a C3 that carries a unchannelized (DS3 clear channel) E3.

### Step 9
**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
Router(config-controller)# au-4 1
Router(config-ctrlr-au4)# mode e3
Router(config-ctrlr-au4)# end
```
Exits controller configuration mode and returns to privileged EXEC mode.

### Command or Action | Purpose
--- | ---
**Step 7**
`au-4 au-4# tug-3 tug-3#`
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.

**Step 8**
`mode e3`
Specifies the mode of operation.

- `e3`—Specifies a C3 that carries a unchannelized (DS3 clear channel) E3.

**Step 9**
`end`
Exits controller configuration mode and returns to privileged EXEC mode.
Optional Configurations

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

- Configuring the Encapsulation Method, page 10-16
- Configuring the CRC Size for T1, page 10-17
- Optional Packet over SONET Configurations, page 10-17

Configuring the Encapsulation Method

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic. To set the encapsulation method, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td>Router(config)# interface serial slot/subslot/port:channel-group</td>
</tr>
<tr>
<td></td>
<td>Selects the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>· slot/subslot/port:channel-group—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Router(config-if)# encapsulation encapsulation-type {hdlc</td>
</tr>
<tr>
<td></td>
<td>Sets the encapsulation method on the interface, where:</td>
</tr>
<tr>
<td></td>
<td>· <strong>hdlc</strong>—Sets the High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces.</td>
</tr>
<tr>
<td></td>
<td>· <strong>ppp</strong>—Sets point-to-point protocol (PPP) for serial interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Frame relay encapsulation is not supported.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 12 Router(config)# interface serial slot/subslot/port:channel-group</td>
<td>Selects the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 13 Router(config-if)# crc {16</td>
<td>32}</td>
</tr>
<tr>
<td></td>
<td>16—16-bit CRC. This is the default.</td>
</tr>
<tr>
<td></td>
<td>32—32-bit CRC.</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, page 10-17
- MTU Value, page 10-18
- Keepalive Value, page 10-18
- Bandwidth, page 10-18
- Scrambling, page 10-18
- C2 Flag, page 10-19
- J1 Flag, page 10-19

Encapsulation

encapsulation encapsulation-type

Example:
Router(config-if)# encapsulation hdlc

Configures encapsulation; you can configure the following options:
- HDLC
- PPP
Chapter 10  Configuring Optical Interface Modules

Optional Configurations

### MTU Value

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtu bytes</td>
<td>Configures the maximum packet size for an interface in bytes. The default packet size is 4470 bytes.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if)# mtu 4000
```

### CRC Value

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crc size-in-bits</td>
<td>CRC size in bits. Valid values are 16 and 32. The default is 16.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if)# crc 32
```

### Keepalive Value

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keepalive [period [retries]]</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• period—Specifies the time interval in seconds for sending keepalive packets. The default is 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if)# keepalive 9 4
```

### Bandwidth

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth {kbps</td>
<td>inherit [kbps]}</td>
</tr>
<tr>
<td></td>
<td>• inherit—Specifies how a subinterface inherits the bandwidth of its main interface.</td>
</tr>
<tr>
<td></td>
<td>• receive—Specifies the receive-side bandwidth.</td>
</tr>
</tbody>
</table>

### 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>pos scramble-atm</td>
<td>Enables scrambling on the interface.</td>
</tr>
</tbody>
</table>
Chapter 10 Configuring Optical Interface Modules

Managing Interface Naming

C2 Flag

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

| pos flag c2 value | Specifies the C2 byte field for the interface as defined in RFC 2615. Valid values are 0-255. |

J1 Flag

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

| pos flag j1 message word | Specifies the value of the J1 byte in the SONET Path OverHead (POH) column. |

You can use the following commands to verify your configuration:

- `show interfaces pos`
- `show controllers 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, page 10-20
- Creating a Multilink Bundle, page 10-20 (required)
- Assigning an Interface to a Multilink Bundle, page 10-21 (required)
- Configuring Fragmentation Size and Delay on an MLPPP Bundle, page 10-21 (optional)
- Disabling Fragmentation on an MLPPP Bundle, page 10-22 (optional)

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.

Creating a Multilink Bundle

To create a multilink bundle, use the following commands:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | Router(config)# interface multilink group-number | Creates a multilink interface and enters multilink interface mode, where:  
| | | • group-number—The group number for the multilink bundle. |
| Step 3 | Router(config-if)# ip address address mask | Sets the IP address for the multilink group, where:  
| | | • address—The IP address.  
| | | • mask—The subnet mask. |
Assigning an Interface to a Multilink Bundle

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config)# interface serial slot/subslot/port</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-if)# encapsulation ppp</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config-if)# ppp multilink group group-number</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Note</td>
</tr>
</tbody>
</table>

Configuring Fragmentation Size and Delay on an MLPPP Bundle

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config)# interface multilink group-number</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-if)# ppp multilink fragment size fragment-size</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config-if)# ppp multilink fragment-delay delay</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following example of the `show ppp multilink` command shows the MLPPP type and the fragmentation size:

```
Router# show ppp multilink
Multilink1, bundle name is test2
Bundle up for 00:00:13
Bundle is Distributed
0 lost fragments, 0 reordered, 0 unassigned
0 discarded, 0 lost received, 206/255 load
0x0 received sequence, 0x0 sent sequence
Member links: 2 active, 0 inactive (max not set, min not set)
```
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:

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

For information about configuring BERT, see “Configuring BERT” section on page 22

Configuring Automatic Protection Switching

For information on how to configure Automatic Protection Switching (APS) on the optical interface module, see Configuring Automatic Protection Switching on the Cisco ASR 900 Series Router.
Chapter 10      Configuring Optical Interface Modules

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.
- `show controllers pos`—Displays status information about the OC POS interface

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# <code>show controller sonet slot/ port-adapter/ port</code></td>
<td>Displays information about the hardware.</td>
</tr>
<tr>
<td>Router# <code>show controllers pos</code></td>
<td>Displays information about the interface.</td>
</tr>
</tbody>
</table>
CHAPTER 10  CONFIGURING OPTICAL INTERFACE MODULES

Configuration Examples

This section includes the following configuration examples:

- Example of Cyclic Redundancy Check Configuration, page 10-24
- Example of Facility Data Link Configuration, page 10-24
- Example of Invert Data on T1/E1 Interface, page 10-24

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 Clocking and Timing

This chapter explains how to configure timing ports on the Route Switch Processor (RSP) modules of the Cisco ASR 900 Series Router and includes the following sections:

- Clocking and Timing Restrictions, page 11-1
- Clocking and Timing Overview, page 11-3
- Configuring Clocking and Timing, page 11-7
- Verifying the Configuration, page 11-37
- Troubleshooting, page 11-38
- Configuration Examples, page 11-39

Clocking and Timing Restrictions

The following clocking and timing restrictions apply to the Cisco ASR 900 Series Router:

- 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 router 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 router 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.
Clocking and Timing Restrictions

- PTP functionality is restricted by license type.

Table 11-1 summarizes the PTP functionalities that are available, by license type:

Table 11-1      PTP Functions Supported by Different Licenses

<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 router to use the full PTP functionality.

- PTP over Ethernet is not supported in multicast mode; only unicast mode is supported.
- End-to-end Transparent Clock is not supported for PTP over Ethernet.
- G.8265.1 telecom profiles are not supported with PTP over Ethernet.
- The Cisco ASR 900 Series Router do 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 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 T_{SM} (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.
Clocking and Timing Overview

The Cisco ASR 900 Series Router 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 Cisco ASR 900 Series Router 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 more information, see the Cisco ASR 903 Hardware Installation Guide.

The following sections describe how to configure clocking and timing features on the Cisco ASR 900 Series Router.

- “Understanding PTP” section on page 3
- “Timing Port Specifications” section on page 6
- “Understanding Synchronous Ethernet ESMC and SSM” section on page 6

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.


Chapter 11 Configuring Clocking and Timing

Clocking and Timing Overview

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” section on page 7.

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 Router supports unicast-based timing as specified in the 1588-2008 standard. Hybrid mode is not supported with PTP 1588 redundancy.

For instructions on how to configure PTP redundancy, see “Configuring PTP Redundancy” section on page 24.

Table 11-2 Nodes within a PTP Network

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grandmaster</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  | 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  | 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. |
| Transparent Clock | 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. |
Hybrid Clocking

The Cisco ASR 900 Series Router 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” section on page 17.

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 Router does not currently support peer-to-peer transparent clock mode.

For information on how to configure the Cisco ASR 900 Series Router as a transparent clock, see “Configuring a Transparent Clock” section on page 16.

Time of Day (TOD)

You can use the time of day (ToD) and 1PPS ports on the Cisco ASR 900 Series Router to exchange ToD clocking. In master mode, the router can receive time of day (ToD) clocking from an external GPS unit; the router requires a ToD, 1PPS, and 10MHZ connection to the GPS unit.

In slave mode, the router 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 Router, see the “Configuring an Ordinary Clock” section on page 8.

Synchronizing the System Clock to Time of Day

You can set the router’s 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” section on page 28.
Timing Port Specifications

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

BITS Framing Support

Table 11-3 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 8, “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 Cisco ASR 900 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.

For more information about Ethernet ESMC and SSM, see “Configuring Synchronous Ethernet ESMC and SSM” section on page 30.

- **Note**: The router 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 Cisco ASR 900 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

Note

You can use override the default clock selection using the commands described in the “Managing Clock Source Selection” section on page 35.

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 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 a equal or higher quality level than the current source.

For more information about how to use these features, see “Managing Clock Source Selection” section on page 35.

Configuring Clocking and Timing

The following sections describe how to configure clocking and timing features on the Cisco ASR 900 Series Router:

- Configuring an Ordinary Clock, page 11-8
- Configuring a Boundary Clock, page 11-14
- Configuring a Transparent Clock, page 11-16
- Configuring a Hybrid Clock, page 11-17
• Configuring PTP Redundancy, page 11-24
• Synchronizing the System Time to a Time-of-Day Source, page 11-28

Configuring an Ordinary Clock

The following sections describe how to configure the Cisco ASR 900 Series Router as an ordinary clock.

• Configuring a Master Ordinary Clock, page 11-8
• Configuring a Slave Ordinary Clock, page 11-11

Configuring a Master Ordinary Clock

Follow these steps to configure the Cisco ASR 900 Series Router to act as a master ordinary clock.

SUMMARY STEPS

1. enable
2. configure terminal
3. ptp clock {ordinary | boundary | e2e-transparent} domain domain-number
4. priority1 priorityvalue
5. priority2 priorityvalue
6. input [1pps] {R0 | R1}
7. tod {R0 | R1} {ubx | nmea | cisco | ntp}
8. clock-port port-name {master | slave} [profile {g8265.1}]
9. transport ipv4 unicast interface interface-type interface-number [negotiation]
   or
   transport ethernet unicast [negotiation]
10. clock destination source-address | mac-address {bridge-domain bridge-domain-id} | interface interface-name
11. sync interval interval
12. announce interval interval
13. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</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 configuration mode. |
| Example: | 
Router# configure terminal |
| Step 3 | ptp clock (ordinary | Configures the PTP clock. You can create the following clock types:  
boundary | ordinary—A 1588 clock with a single PTP port that can operate in  
e2e-transparent | boundary—Terminates PTP session from Grandmaster and acts as  
domain-number | PTP master to slaves downstream.  
domain 0--- | 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  
Router(config-ptp-clk)# |
| Step 4 | priority1 priorityvalue | 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. |
| Example: | 
Router(config-ptp-clk)# priority1 priorityvalue |
| Step 5 | priority2 priorityvalue | 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 router is unable to use priority1 and other clock attributes to select a clock.  
Valid values are from 0-255. The default value is 128. |
| Example: | 
Router(config-ptp-clk)# priority2 priorityvalue |
| Step 6 | 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. |
| Example: | 
Router(config-ptp-clk)# input 1pps R0 |
| Step 7 | 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-ptp-clk)# tod R0 ntp |
## Configuring Clocking and Timing

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock-port port-name {master | slave} [profile {g8265.1}]</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ptp-clk)# clock-port Master master Router(config-ptp-port)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>transport ipv4 unicast interface interface-type interface-number [negotiation] or transport ethernet unicast [negotiation]</td>
<td>Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport. 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.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock destination source-address | mac-address {bridge-domain bridge-domain-id} | interface interface-name}</td>
<td>Specifies the IP address or MAC address of a clock destination when the router is in PTP master mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ptp-port)# clock-source 8.8.8.1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>sync interval interval</td>
<td>Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values, as follows:</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ptp-port)# sync interval -4</td>
<td></td>
</tr>
<tr>
<td>- 1—1 packet every 2 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- 0—1 packet every second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- -1—1 packet every 1/2 second, or 2 packets per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- -2—1 packet every 1/4 second, or 4 packets per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- -3—1 packet every 1/8 second, or 8 packets per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- -4—1 packet every 1/16 seconds, or 16 packets per second.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- -5—1 packet every 1/32 seconds, or 32 packets per second.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- -6—1 packet every 1/64 seconds, or 64 packets per second.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- -7—1 packet every 1/128 seconds, or 128 packets per second.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Slave Ordinary Clock

Follow these steps to configure the Cisco ASR 900 Series Router 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}`
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]`
   or
   `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`

---

**Step 12**

**Command:**

`announce interval interval`

**Example:**

```
Router(config-ptp-port)# announce interval 2
```

**Purpose:**

- Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows:
  - `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 13**

**Command:**

`end`

**Example:**

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

**Purpose:**

- Exit configuration mode.
## Configuring Clocking and Timing

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable  | Enables privileged EXEC mode.  
      |         | • Enter your password if prompted. |
| 2    | configure terminal | Enter configuration mode. |
| 3    | ptp clock {ordinary | Configures the PTP clock. You can create the following clock types:  
      | boundary | • ordinary—A 1588 clock with a single PTP port that can operate in  
      |  e2e-transparent | Master or Slave mode.  
      | domain-number [hybrid] | • 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. |
| 4    | output [1pps] {R0 | Enables Precision Time Protocol input 1PPS using a 1PPS input port. 
      | R1} | Use R0 or R1 to specify the active RSP slot. |
| 5    | tod {R0 | Configures the time of day message format used by the ToD interface.  
      | R1} | Note The ToD port acts as an input port in case of Master clock and as  
      | {ubx | an output port in case of Slave clock. |
      | nmea |  
      | cisco |  
      | ntp} |  
| 6    | clock-port port-name {master | Sets the clock port to PTP master or slave mode; in slave mode, the port  
      | slave | exchanges timing packets with a PTP master clock.  
      | [profile | The profile keyword configures the clock to use the G.8265.1  
      | g8265.1]} | 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:**

```plaintext
Router> enable
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# output 1pps R0
Router(config-ptp-clk)# tod R0 ntp
Router(config-ptp-clk)# clock-port slave
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 7       | `transport ipv4 unicast interface`                         | Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.  
|         | `interface-type interface-number [negotiation]`             | The negotiation keyword configures the router to discover a PTP master clock from all available PTP clock sources.  
|         | or                                                          | Note PTP redundancy is supported only on unicast negotiation mode.       |
|         | `transport ethernet unicast [negotiation]`                  |                                                                        |
|         | Example:                                                     | `Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation` |
| 8       | `clock source source-address | mac-address {bridge-domain bridge-domain-id} | interface interface-name} [priority]` | Specifies the IP or MAC address of a PTP master clock.                   |
|         | Example:                                                     | `Router(config-ptp-port)# clock-source 8.8.8.1`                        |
| 9       | `announce timeout value`                                    | Specifies the number of PTP announcement intervals before the session times out. Valid values are 1-10. |
|         | Example:                                                     | `Router(config-ptp-port)# announce timeout 8`                          |
| 10      | `delay-req interval interval`                               | Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.  
|         | Example:                                                     | `Router(config-ptp-port)# delay-req interval 1`                        |
|         |                                                               | The intervals are set using log base 2 values, as follows:              |
|         |                                                               | • 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`                                          |
Configuring a Boundary Clock

Follow these steps to configure the Cisco ASR 900 Series Router to act as a boundary clock.

**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]`
6. `clock-source source-address [priority]`
7. `clock-port port-name {master | slave} [profile {g8265.1}]`
8. `transport ipv4 unicast interface interface-type interface-number [negotiation]`
9. `end`
## Chapter 11 Configuring Clocking and Timing

### Configuring Clocking and Timing

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config)# ptp clock {ordinary</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ptp clock boundary domain 0</td>
</tr>
<tr>
<td></td>
<td>Configures the PTP clock. You can create the following clock types:</td>
</tr>
<tr>
<td></td>
<td>• ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.</td>
</tr>
<tr>
<td></td>
<td>• boundary—Terminates PTP session from Grandmaster and acts as PTP master to slaves downstream.</td>
</tr>
<tr>
<td></td>
<td>• e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at slave.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>clock-port port-name {master</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-tpg-clk)# clock-port SLAVE slave</td>
</tr>
<tr>
<td></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></td>
<td>The profile keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Using a telecom profile requires that the clock have a domain number of 4–23.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>transport ipv4 unicast interface interface-type interface-number [negotiation]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-tpg-port)# transport ipv4 unicast interface Loopback 0 negotiation</td>
</tr>
<tr>
<td></td>
<td>Specifies the transport mechanism for clocking traffic.</td>
</tr>
<tr>
<td></td>
<td>The negotiation keyword configures the router to discover a PTP master clock from all available PTP clock sources.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>PTP redundancy is supported only on unicast negotiation mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>clock-source source-address [priority]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-tpg-port)# clock source 133.133.133.133</td>
</tr>
<tr>
<td></td>
<td>Specifies the address of a PTP master clock. You can specify a priority value as follows:</td>
</tr>
<tr>
<td></td>
<td>• No priority value—Assigns a priority value of 0.</td>
</tr>
<tr>
<td></td>
<td>• 1—Assigns a priority value of 1.</td>
</tr>
<tr>
<td></td>
<td>• 2—Assigns a priority value of 2, the highest priority.</td>
</tr>
</tbody>
</table>
Configuring Clocking and Timing

Chapter 11  Configuring Clocking and Timing

Configuring a Transparent Clock

Follow these steps to configure the Cisco ASR 900 Series Router as an end-to-end transparent clock.

Note

The Cisco ASR 900 Series Router does not support peer-to-peer transparent clock mode.

Note

The transparent clock ignores the domain number.

SUMMARY STEPS

1. enable
2. configure terminal
3. ptp clock e2e-transparent domain domain-number
4. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</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 | Enter configuration mode. |
| Example: | Router# configure terminal |
| **Step 3** | ptp clock (ordinary | Configures the router as an end-to-end transparent clock.  
  boundary |  
  e2e-transparent) domain  
  domain-number [hybrid] |
| Example: | Router(config)# ptp clock  
  e2e-transparent domain 4 |
| **Step 4** | exit | Exit configuration mode. |
| Example: | Router(config)# exit |

### Configuring a Hybrid Clock

The following sections describe how to configure the Cisco ASR 900 Series Router to act as a hybrid clock.

- Configuring a Hybrid Boundary Clock, page 11-17
- Configuring a Hybrid Ordinary Clock, page 11-21

### 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 (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]
6. `clock-source source-address [priority]`
7. `clock-port port-name {master | slave} [profile {g8265.1}]`
8. `transport ipv4 unicast interface interface-type interface-number [negotiation]`
9. `exit`
10. 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>`
11. `network-clock synchronization mode ql-enabled`
12. `network-clock hold-off [0 | milliseconds]`
13. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</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>
<tr>
<td>Example: Router(config)# ptp clock boundary domain 0 hybrid</td>
<td>• <strong>ordinary</strong>—A 1588 clock with a single PTP port that can operate in Master or Slave mode.</td>
</tr>
<tr>
<td><strong>Note</strong> Hybrid mode is only supported with slave clock-ports; master mode is not supported.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ptp clock {ordinary</td>
<td>boundary</td>
</tr>
<tr>
<td>Example: Router(config)# ptp clock boundary domain 0 hybrid</td>
<td>• <strong>boundary</strong>—Terminates PTP session from Grandmaster and acts as PTP master to slaves downstream.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ptp clock {ordinary</td>
<td>boundary</td>
</tr>
<tr>
<td>Example: Router(config)# ptp clock boundary domain 0 hybrid</td>
<td>• <strong>e2e-transparent</strong>—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>
</tbody>
</table>
## Chapter 11 Configuring Clocking and Timing

### Step 4: `clock-port port-name {master | slave} [profile {g8265.1}]`

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

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

**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.

### Step 5: `transport ipv4 unicast interface [negotiation]`

**Purpose:** Specifies the transport mechanism for clocking traffic.

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

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

### Step 6: `clock-source source-address [priority]`

**Purpose:** 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-pts-port)# clock-source 133.133.133.133
```

### Step 7: `clock-port port-name {master | slave} [profile {g8265.1}]`

**Purpose:** Sets the clock port to PTP master or slave mode; in master mode, the port exchanges timing packets with PTP slave devices.

**Example:**
```
Router(config-pts-port)# clock-port
MASTER master
```

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 8: `transport ipv4 unicast interface [negotiation]`

**Purpose:** Specifies the transport mechanism for clocking traffic.

**Example:**
```
Router(config-pts-port)# transport ipv4 unicast interface Lo1 negotiation
```

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

### Step 9: `exit`

**Purpose:** Exit clock-port configuration.
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 10 | 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 [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 BITS port as network clock input source in t1 mode.  
- (Optional) To nominate Ethernet interface as network clock input source.

| Step 11 | `network-clock synchronization mode ql-enabled` | Enables automatic selection of a clock source based on quality level (QL).  
**Note** This command is disabled by default.  
For more information about this command, see Chapter 11, “Configuring Clocking and Timing.” |

| Step 12 | `network-clock hold-off [0 | milliseconds]` | (Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.  
**Note** You can also specify a hold-off value for an individual interface using the `network-clock hold-off` command in interface mode.  
For more information about this command, see Chapter 11, “Configuring Clocking and Timing.” |

| Step 13 | `end` | Exit configuration mode. |

*Example:*  
`Router(config)# end`
Configuring a Hybrid Ordinary Clock

Follow these steps to configure a hybrid clocking in ordinary clock slave 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 [ordinary | boundary | e2e-transparent] domain domain-number [hybrid]
4. output [1pps] {R0 | R1}
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. 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>
11. network-clock synchronization mode ql-enabled
12. network-clock hold-off {0 | milliseconds}
13. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</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>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></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>Example:</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>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ptp clock ordinary domain 0 hybrid</code></td>
<td>• <strong>ordinary</strong>—A 1588 clock with a single PTP port that can operate in</td>
</tr>
<tr>
<td></td>
<td>Master or Slave mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>boundary</strong>—Terminates PTP session from Grandmaster and acts as</td>
</tr>
<tr>
<td></td>
<td>PTP master to slaves downstream.</td>
</tr>
<tr>
<td></td>
<td>• <strong>e2e-transparent</strong>—Updates the PTP time correction field to account</td>
</tr>
<tr>
<td></td>
<td>for the delay in forwarding the traffic. This helps improve the</td>
</tr>
<tr>
<td></td>
<td>accuracy of 1588 clock at slave.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>`output [1pps] {R0</td>
<td>R1}`</td>
</tr>
<tr>
<td>Example:</td>
<td>Use R0 or R1 to specify the active RSP slot.</td>
</tr>
<tr>
<td><code>Router(config-ptp-clk)# output 1pps R0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>`tod {R0</td>
<td>R1} {ubx</td>
</tr>
<tr>
<td>Example:</td>
<td>The ToD port acts as an input port in case of Master clock and as an</td>
</tr>
<tr>
<td><code>Router(config-ptp-clk)# tod R0 ntp</code></td>
<td>output port in case of Slave clock.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>`clock-port port-name {master</td>
<td>slave} [profile {g8265.1}]`</td>
</tr>
<tr>
<td>Example:</td>
<td>port exchanges timing packets with a PTP master clock.</td>
</tr>
<tr>
<td><code>Router(config-ptp-clk)# clock-port SLAVE slave</code></td>
<td>• <strong>Ordinary</strong>—A 1588 clock with a single PTP port that can operate in</td>
</tr>
<tr>
<td></td>
<td>Master or Slave mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Boundary</strong>—Terminates PTP session from Grandmaster and acts as</td>
</tr>
<tr>
<td></td>
<td>PTP master to slaves downstream.</td>
</tr>
<tr>
<td></td>
<td>• <strong>E2e-transparent</strong>—Updates the PTP time correction field to account</td>
</tr>
<tr>
<td></td>
<td>for the delay in forwarding the traffic. This helps improve the</td>
</tr>
<tr>
<td></td>
<td>accuracy of 1588 clock at slave.</td>
</tr>
<tr>
<td></td>
<td>Note Hybrid mode is only supported with slave clock-ports; master</td>
</tr>
<tr>
<td></td>
<td>mode is not supported.</td>
</tr>
<tr>
<td></td>
<td>Note Using a telecom profile requires that the clock have a domain</td>
</tr>
<tr>
<td></td>
<td>number of 4–23.</td>
</tr>
</tbody>
</table>
### Step 7
**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 router to discover a PTP master clock from all available PTP clock sources.

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

### Step 8
**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.

### Step 9
**exit**

**Example:**
```
Router(config-ptp-port)# exit
```

Exit clock-port configuration.

### Step 10
Use one of the following options:

- **network-clock input-source**
  - `<priority>` controller {SONET | wanphy}
  - `external` {R0 | R1} [10m | 2m]
  - `external` {R0 | R1} [2048k | e1 {cas 120ohms | 75ohms | crc4}]}
  - `external` {R0 | R1} [2048k | e1 {crc4 | fas | 120ohms | 75ohms} {linecode {ami | hdb3}}]
  - `external` {R0 | R1} [t1 {d4 | esf | sf} {linecode {ami | b8zs}}]
  - `interface` <type/slot/port>

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

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.
Chapter 11  Configuring Clocking and Timing

Configuring PTP Redundancy

The following sections describe how to configure PTP redundancy on the Cisco ASR 900 Series Router:

- Configuring PTP Redundancy in Slave Clock Mode, page 11-24
- Configuring PTP Redundancy in Boundary Clock Mode, page 11-26

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 domain domain-number
4. clock-port port-name slave [profile {g8265.1}]
5. transport ipv4 unicast interface interface-type interface-number [negotiation]
6. clock-source source-address [priority]
7. clock-source source-address [priority]
8. clock-source source-address [priority]
9. end

---

**Command Purpose**

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>network-clock synchronization mode ql-enabled</td>
<td>Enables automatic selection of a clock source based on quality level (QL).</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router(config-ptp-clk)#网络-clock synchronization mode ql-enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This command is disabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about this command, see Chapter 11, “Configuring Clocking and Timing.”</td>
</tr>
</tbody>
</table>

| Step 12          | network-clock hold-off {0 | milliseconds} | (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. |
|                  | Example:                                     | Router(config-ptp-clk)#network-clock hold-off 0                          |
|                  |                                              | 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 Chapter 11, “Configuring Clocking and Timing.” |

| Step 13          | end                                           | Exit configuration mode.                                               |
|                  | Example:                                     | Router(config-ptp-clk)# end                                             |
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</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 | Enter configuration mode. |
| Example: | Router# configure terminal |
| Step 3 | 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 | 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-tpc-clk)# clock-port SLAVE slave |
| Step 5 | 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. |
| Example: | Router(config-tpc-port)# transport ipv4 unicast interface Loopback 0 negotiation |
| Step 6 | 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-tpc-port)# clock source 133.133.133.133 1 |
| Step 7 | clock-source source-address [priority] | 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. |
| Example: | Router(config-tpc-port)# clock source 133.133.133.134 2 |
Configuring Clocking and Timing

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 \[ negotiation \]
6. clock-source source-address \[ priority \]
7. clock-source source-address \[ priority \]
8. clock-source source-address \[ priority \]
9. clock-port port-name master \[ profile \{ g8265.1 \}\]
10. transport ipv4 unicast interface interface-type interface-number \[ negotiation \]
11. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 3    | ptp clock {ordinary | boundary | e2e-transparent} domain domain-number | 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. |
| 4    | 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. |
| 5    | 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. |
| 6    | 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. |
| 7    | clock-source source-address [priority] | 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. |
| 8    | clock-source source-address [priority] | 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. |
| 9    | clock-port port-name [master | slave] [profile {g8265.1}] | 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. |
### Configuring Clocking and Timing

#### 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, page 11-8. 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>Transport</strong> ipv4 unicast interface interface-type interface-number [negotiation]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ptp-port)# end</td>
</tr>
</tbody>
</table>

### 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), page 11-28
- Synchronizing the System Time to a Time-of-Day Source (Slave Mode), page 11-29

#### Synchronizing the System Time to a Time-of-Day Source (Master Mode)
## Chapter 11 Configuring Clocking and Timing

### Configuring Clocking and Timing

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>tod-clock input-source priority {gps {R0</td>
<td>R1}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>tod-clock input-source priority {gps {R0</td>
<td>R1}</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exit configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>exit</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, page 11-11.

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. exit
**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 Cisco ASR 900 Series Router.

- Configuring Synchronous Ethernet ESMC and SSM, page 11-30
- Managing Clock Source Selection, page 11-35

**Configuring Synchronous Ethernet ESMC and SSM**

Follow these steps to configure ESMC and SSM on the Cisco ASR 900 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. Use one of the following options:
   - network-clock input-source <priority> controller {SONET | wanphy}
   - network-clock input-source <priority> external {R0 | R1} [10m | 2m]
- \texttt{network-clock input-source <priority> external [R0 \ R1] [2048k \ e1 \ {cas [120ohms \ 75ohms \ | \ crc4]}}]
- \texttt{network-clock input-source <priority> external [R0 \ R1] [2048k \ e1 \ {crc4 \ fas] \ {120ohms \ 75ohms} \ {linecode {ami \ hdb3}}]}
- \texttt{network-clock input-source <priority> external [R0 \ R1] [t1 \ {d4 \ esf \ sf] \ {linecode {ami \ b8zs}}]}
- \texttt{network-clock input-source <priority> interface <type/slot/port>}
- \texttt{network-clock input-source <priority> ptp domain <domain-number>}
- \texttt{network-clock synchronization mode ql-enabled}
- \texttt{network-clock hold-off \{0 \ milliseconds\}}
- \texttt{network-clock wait-to-restore seconds}
- \texttt{network-clock revertive}
- \texttt{esmc process}
- \texttt{network-clock external slot/card/port hold-off \{0 \ milliseconds\}}
- \texttt{network-clock quality-level \{tx \ rx\} value \{controller [E1\ BITS] slot/card/port \ external [2m \ 10m \ 2048k \ t1 \ e1] \}}
- \texttt{interface type number}
- \texttt{synchronous mode}
- \texttt{network-clock source quality-level value \{tx \ rx\}}
- \texttt{esmc mode \{ql-disabled \ tx \ rx\} value}
- \texttt{network-clock hold-off \{0 \ milliseconds\}}
- \texttt{network-clock wait-to-restore seconds}
- \texttt{end}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</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** 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 | |
### Chapter 11      Configuring Clocking and Timing

#### Step 4
**network-clock eec {1 | 2}**

**Example:**
Router(config)# network-clock eec 1

Specifies the Ethernet Equipment Clock (EEC) type. Valid values are

- 1—ITU-T G.8262 option 1 (2048)
- 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544)

#### Step 5
**network-clock synchronization ssm option {1 | 2 [GEN1 | GEN2]}**

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

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>**
- **network-clock input-source <priority> ptp domain <domain-number>**

**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 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 PTP as network clock input source.

#### Step 7
**network-clock synchronization mode ql-enabled**

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

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

**Note** This command is disabled by default.
### Chapter 11      Configuring Clocking and Timing

#### Configuring Clocking and Timing

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8</td>
<td>network-clock hold-off {0</td>
<td>milliseconds}</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock hold-off 0</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>network-clock wait-to-restore seconds</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. &lt;br&gt;Valid values are 0 to 86400 seconds. The default value is 300 seconds. &lt;br&gt;&lt;br&gt;Note: You can also specify a wait-to-restore value for an individual interface using the <code>network-clock wait-to-restore</code> command in interface mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock wait-to-restore 70</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>network-clock revertive</td>
<td>(Optional) Sets the router in revertive switching mode when recovering from a failure. To disable revertive mode, use the <code>no</code> form of this command.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock revertive</td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td>esmc process</td>
<td>Enables the ESMC process globally.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# esmc process</td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td>network-clock external slot/card/port hold-off {0</td>
<td>milliseconds}</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock external 0/1/0 hold-off 0</td>
<td></td>
</tr>
<tr>
<td>Step 13</td>
<td>network-clock quality-level {tx</td>
<td>rx} value {controller [E1</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock quality-level rx ql-pRC external R0 e1 cas crc4</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Clocking and Timing

#### Step 14
**command:** `interface type number`
- **Purpose:** Enters interface configuration mode.
- **Example:**
  ```
  Router(config)# interface GigabitEthernet 0/0/1
  Router(config-if)#
  ```

#### Step 15
**command:** `synchronous mode`
- **Purpose:** Configures the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface.
- **Example:**
  ```
  Router(config-if)# synchronous mode
  ```

#### Step 16
**command:** `network-clock source quality-level value {tx | rx}`
- **Purpose:** Applies quality level on sync E interface.
- **Example:**
  ```
  Router(config-if)# network-clock source quality-level QL-PrC tx
  ```

#### Step 17
**command:** `esmc mode [ql-disabled | tx | rx] value`
- **Purpose:** Enables the ESMC process at the interface level. The `no` form of the command disables the ESMC process.
- **Example:**
  ```
  Router(config-if)# esmc mode rx QL-STU
  ```

#### Step 18
**command:** `network-clock hold-off [0 | milliseconds]`
- **Purpose:** (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.
- **Example:**
  ```
  Router(config-if)# network-clock hold-off 0
  ```

#### Step 19
**command:** `network-clock wait-to-restore seconds`
- **Purpose:** (Optional) Configures the wait-to-restore timer for an individual synchronous Ethernet interface.
- **Example:**
  ```
  Router(config-if)# network-clock wait-to-restore 70
  ```

#### Step 20
**command:** `end`
- **Purpose:** Exits interface configuration mode and returns to privileged EXEC mode.
- **Example:**
  ```
  Router(config-if)# end
  ```

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 Cisco ASR 900 Series Router:

- Specifying a Clock Source, page 11-35
- Disabling a Clock Source, page 11-36

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, page 11-35
- Forcing a Clock Source Selection, page 11-35
- Disabling Clock Source Specification Commands, page 11-36

Selecting a Specific Clock Source

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

Note: The new clock source must be of higher quality than the current clock source; otherwise the router 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>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# network-clock switch manual external r0 e1 crc4</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.
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>Example:</td>
<td>Router# network-clock clear switch t0</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, page 11-36
- Restoring a Clock Source, page 11-37

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.
Command | Purpose
--- | ---
network-clock set lockout (interface interface_name slot/card/port | external | R0 | R1 | ( t1 | sf | esf | linecode (ami | b8zs)) | e1 [crc4 | fas] linecode [hdb3 | ami]) | Prevents the router from selecting a specific synchronous Ethernet clock source.

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

network-clock clear lockout (interface interface_name slot/card/port | external | R0 | R1 | ( t1 | sf | esf | linecode (ami | b8zs)) | e1 [crc4 | fas] linecode [hdb3 | ami]) | Disable a lockout configuration on a synchronous Ethernet clock source.

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

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

Command | Purpose
--- | ---
network-clock clear lockout (interface interface_name slot/card/port | external | R0 | R1 | ( t1 | sf | esf | linecode (ami | b8zs)) | e1 [crc4 | fas] linecode [hdb3 | ami]) | Forces the router to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.

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

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

- **show esmc**—Displays the ESMC configuration.
- **show esmc detail**—Displays the details of the ESMC parameters at the global and interface levels.
- **show network-clock synchronization**—Displays the router 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 11-4 list the debug commands that are available for troubleshooting the SyncE configuration on the Cisco ASR 900 Series Router:

⚠️ Caution

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

Table 11-4  SyncE Debug Commands

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

Table 11-5 provides the information about troubleshooting your configuration
Table 11-5  Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock selection</td>
<td>• Verify that there are no alarms on the interfaces using the <code>show network-clock synchronization detail</code> 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 <code>debug network-clock errors</code>, <code>debug network-clock event</code>, and <code>debug network-clock sm</code> commands. Contact Cisco Technical Support if the issue persists.</td>
</tr>
<tr>
<td>Incorrect QL values</td>
<td>• Ensure that there is no framing mismatch with the SSM option.</td>
</tr>
<tr>
<td></td>
<td>• Reproduce the issue using the <code>debug network-clock errors</code> and <code>debug network-clock event</code> commands.</td>
</tr>
<tr>
<td>Alarms</td>
<td>• Reproduce the issue using the <code>debug platform network-clock</code> command enabled in the RSP. Alternatively, enable the <code>debug network-clock event</code> and <code>debug network-clock errors</code> commands.</td>
</tr>
<tr>
<td>Incorrect clock limit set or queue limit</td>
<td>• Verify that there are no alarms on the interfaces using the <code>show network-clock synchronization detail</code> command.</td>
</tr>
<tr>
<td>disabled mode</td>
<td>• Use the <code>show network-clock synchronization</code> command to confirm if the system is in revertive 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 <code>debug network-clock errors</code>, <code>debug network-clock event</code>, and <code>debug network-clock sm</code> RSP commands.</td>
</tr>
<tr>
<td>Incorrect QL values when you use the <code>show</code></td>
<td>• Use the <code>network clock synchronization SSM</code> *(option 1</td>
</tr>
<tr>
<td>network-clock synchronization detail` command.</td>
<td>For the SSM option 1, framing should be SDH or E1, and for SSM option 2, it should be T1.</td>
</tr>
<tr>
<td></td>
<td>• Reproduce the issue using the <code>debug network-clock errors</code> and <code>debug network-clock event</code> RSP commands.</td>
</tr>
</tbody>
</table>

Configuration Examples

This section contains sample configurations for clocking features on the Cisco ASR 900 Series Router.

Note

This section contains partial router configurations intended to demonstrate a specific feature.

Ordinary Clock—Slave

```
ptp clock ordinary domain 0
clock-port Slave slave
transport ipv4 unicast interface loopback 0 negotiation
clock-source 8.8.8.1
announce timeout 7
delay-req interval 100
```
Ordinary Clock — Slave Mode (Ethernet)

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

Ordinary Clock — Master

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

Ordinary Clock — Master (Ethernet)

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

Unicast Configuration — Slave Mode

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

Unicast Configuration — Slave Mode (Ethernet)

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

Unicast Configuration — Master Mode

```
ptp clock ordinary domain 0
clock-port Master master
transport ipv4 unicast interface loopback 0
clock-destination 8.8.8.2
sync interval 1
announce interval 2
```

Unicast Configuration — Master Mode (Ethernet)

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

Unicast Negotiation — Slave

```
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

```plaintext
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

```plaintext
ptp clock e2e-transparent domain 0
```

Hybrid Clock—Boundary

```plaintext
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

```plaintext
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

```plaintext
ptp clock ordinary domain 0
```
Configuration Examples

Chapter 11     Configuring Clocking and Timing

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

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

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
clock-port SLA slave
transport ipv4 unicast interface loopback 0 negotiation
clock source 33.1.1.

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

Router# show ptp clock running domain 0
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>
<tr>
<td>8.8.8.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SESSION INFORMATION

SLAVE [Lo0] [Sessions 1]

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

Router#

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]

--------------------------------
| clock role      | SLAVE     |
| Slave Port hdl  | 486539266 |
| Tx Mode         | Unicast-Negotiation |
| Slave IP        | 4.4.4.4   |
| Max Clk Srcs    | 1         |
| Boundary Clock  | FALSE     |
| Lock status     | HOLDOVER  |
| Refcnt          | 1         |
| Configured-Flags| 0x7F - Clock Port Stream |
| Config-Ready-Flags| Port Stream |
--------------------------------
| PTP Engine Handle| 0         |
| Master IP       | 8.8.8.8   |
| Local Priority  | 0         |
| Set Master IP   | 8.8.8.8   |
Router# `show platform ptp tod all`
--------------------------------
ToD/1PPS 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]

<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>PHASE_ALIGNED</td>
<td>2</td>
<td>32355</td>
<td>159516</td>
<td>Hot standby</td>
</tr>
</tbody>
</table>

PORT SUMMARY

PTP Master

<table>
<thead>
<tr>
<th>Name</th>
<th>Tx Mode</th>
<th>Role</th>
<th>TransportState</th>
<th>Sessions</th>
<th>Port Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLAVE</td>
<td>unicast</td>
<td>slave</td>
<td>Ethernet</td>
<td>1</td>
<td>9.9.9.1</td>
</tr>
<tr>
<td>MASTER</td>
<td>unicast</td>
<td>master</td>
<td>Ethernet -</td>
<td>2</td>
<td>-</td>
</tr>
</tbody>
</table>

SESSION INFORMATION

SLAVE [Ethernet] [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>9.9.9.1</td>
<td>159083</td>
<td>31054</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

MASTER [Ethernet] [Sessions 2]

<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>aabb.ccdd.ee01 [Gig0/2/3]</td>
<td>223</td>
<td>667</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aabb.ccdd.ee02 [BD 1000]</td>
<td>210</td>
<td>634</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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.

```
! 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
```
Configuring Pseudowire

This chapter provides information about configuring pseudowire (PW) features on the Cisco ASR 903 Series Router. It contains the following sections:

- Pseudowire Overview, page 12-1
- Configuring CEM, page 12-5
- Configuring Structure-Agnostic TDM over Packet (SAToP), page 12-13
- Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN), page 12-14
- Configuring an ATM over MPLS Pseudowire, page 12-16
- Configuring an Ethernet over MPLS Pseudowire, page 12-23
- Configuring Pseudowire Redundancy, page 12-25
- Verifying the Interface Configuration, page 12-27
- Configuration Examples, page 12-28

Pseudowire Overview

The following sections provide an overview of pseudowire support on the Cisco ASR 903 Series Router.

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.
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 bit stream. 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 12-1 shows the frame format in Unstructured SAToP mode.

![Figure 12-1 Unstructured SAToP Mode Frame Format](image)

Table 12-1 shows the payload and jitter limits for the T1 lines in the SAToP frame format.

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

Table 12-2 shows the payload and jitter limits for the E1 lines in the SAToP frame format.

<table>
<thead>
<tr>
<th>Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</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>
</tr>
</tbody>
</table>

For instructions on how to configure SAToP, see “Configuring Structure-Agnostic TDM over Packet (SAToP)” section on page 12-13.
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.

CESoPSN supports channel associated signaling (CAS) for E1 and T1 interfaces. CAS provides signaling information within each DS0 channel as opposed to using a separate signaling channel. CAS is also referred to as in-band signaling or robbed bit signaling.

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

*Figure 12-2* shows the frame format in CESoPSN mode.

*Figure 12-2 Structured CESoPSN Mode Frame Format*

<table>
<thead>
<tr>
<th>Encapsulation header</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE Control (4Bytes)</td>
</tr>
<tr>
<td>RTP (optional 12B)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>CEsoP Payload</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Frame#1</td>
</tr>
<tr>
<td>Timeslots 1-N</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Frame#2</td>
</tr>
<tr>
<td>Timeslots 1-N</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Frame#3</td>
</tr>
<tr>
<td>Timeslots 1-N</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Frame#m</td>
</tr>
<tr>
<td>Timeslots 1-N</td>
</tr>
</tbody>
</table>

*Table 12-3 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>
</tbody>
</table>
Pseudowire Overview

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

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.

<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>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>
<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>
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” section on page 12-16.

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.

For instructions on how to create an EoMPLS PW, see Configuring an Ethernet over MPLS Pseudowire, page 12-23.

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:

- Configuration Guidelines and Restrictions, page 12-6
- Configuring a CEM Group, page 12-6
- Using CEM Classes, page 12-7
- Configuring CEM Parameters, page 12-8

Note

Steps for configuring CEM features are also included in the Configuring Structure-Agnostic TDM over Packet (SAToP) and Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN) 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</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td>Step 3</td>
<td>controller {t1</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
</tbody>
</table>
Chapter 12 Configuring Pseudowire

Configuring CEM

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.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 ( \text{enable} )</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 ( \text{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 3 ( \text{Router(config)# class cem mycemclass} )</td>
<td>Creates a new CEM class</td>
</tr>
</tbody>
</table>
### Configuring CEM Parameters

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

- Configuring Payload Size (Optional), page 12-8
- Setting the Dejitter Buffer Size, page 12-9
- Setting an Idle Pattern (Optional), page 12-9
- Enabling Dummy Mode, page 12-9
- Setting a Dummy Pattern, page 12-9
- Shutting Down a CEM Channel, page 12-9

**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 `payload-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
Chapter 12  Configuring Pseudowire

Configuring CEM

- 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
```

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 ATM

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

- Configuring a Clear-Channel ATM Interface, page 12-10
- Configuring ATM IMA, page 12-10

Configuring a Clear-Channel ATM Interface

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.
- Enter your password if prompted.

| Step 2  | configure terminal |

**Example:**

```
Router# configure terminal
```

Enters global configuration mode.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Router(config)# controller {t1} slot/subslot/port</th>
</tr>
</thead>
</table>

Selects the T1 controller for the port you are configuring (where slot/subslot identifies the location and port identifies the port).

| Step 2  | Router(config-controller)# atm |

Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is atm/slot/subslot/port.

**Note** The slot number is always 0.

| Step 3  | Router(config-controller)# end |

Exits configuration mode.

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 Chapter 12, “Configuring Pseudowire.”

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 Chapter 12, “Configuring Pseudowire.”
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 3.

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>Command</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>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`card type {t1</td>
<td>e1} slot [bay]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# card type e1 0 0</td>
<td></td>
</tr>
</tbody>
</table>
### Step 4

**Command**

```plaintext
controller \( \{t1 \mid e1\} \) slot/subslot/port
```

**Purpose**

Specifies the controller interface on which you want to enable IMA.

**Example:**

```
Router(config)# controller E1 0/0/4
Router(config-controller)#
```

---

### Step 5

**Command**

```plaintext
clock source internal
```

**Purpose**

Sets the clock source to internal.

**Example:**

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

---

### Step 6

**Command**

```plaintext
ima group group-number
```

**Purpose**

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.

**Example:**

```
Router(config-controller)# ima-group 0 scrambling-payload
```

**Note** This command automatically creates an ATM0/IMAx interface.

---

### Step 7

**Command**

```plaintext
exit
```

**Purpose**

To add another member link, repeat Step 3 to Step 6.

**Example:**

```
Router(config-controller)# exit
```

---

### Step 8

**Command**

```plaintext
interface ATM slot/subslot/IMA group-number
```

**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.

**Example:**

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

**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 10

**Command**

```plaintext
no ip address
```

**Purpose**

Disables the IP address configuration for the physical layer interface.

**Example:**

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

---

### Step 11

**Command**

```plaintext
atm bandwidth dynamic
```

**Purpose**

Specifies the ATM bandwidth as dynamic.

**Example:**

```
Router(config-if)# atm bandwidth dynamic
```
Configuring Structure-Agnostic TDM over Packet (SAToP)

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

<table>
<thead>
<tr>
<th>Command</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>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 3 controller [T1</td>
<td>E1] 0/4</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 4 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>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 5 Router(config)# interface CEM0/4</td>
<td>Defines a CEM group.</td>
</tr>
<tr>
<td>Router(config-if)# no ip address</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# cem 4</td>
<td></td>
</tr>
</tbody>
</table>
# Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)

Follow these steps to configure CESoPSN on the Cisco ASR 903 Series Router.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Router(config)# controller [e1</td>
<td>t1] 0/0 Router(config-controller)#</td>
</tr>
<tr>
<td><strong>Step 4</strong> Router(config-controller)# cem-group 5 timeslots 1-24</td>
<td>Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the <code>timeslots</code> parameter to assign specific timeslots to the CEM channel.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Router(config-controller)# exit Router(config)#</td>
<td>Exits controller configuration.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Router(config)# interface CEM0/5 Router(config-if-cem)# cem 5</td>
<td>Defines a CEM channel.</td>
</tr>
</tbody>
</table>

---

**Note:** When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as `ip route 30.30.30.2 255.255.255.255 1.2.3.4`.

---

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> Router(config-if)# xconnect 30.30.30.2 304 encapsulation mpls</td>
<td>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 30.30.2.304.</td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# exit Router#</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Clear-Channel ATM Pseudowire

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>Router(config)# controller {t1} slot/subslot/port</code></td>
<td>Selects the T1 controller for the port you are configuring.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>The slot number is always 0.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>Router(config-controller)# 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></td>
<td><strong>Note</strong></td>
<td>The slot number is always 0.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>Router(config-controller)# exit</code></td>
<td>Returns you to global configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>Router(config)# interface atm/slot/subslot/port</code></td>
<td>Selects the ATM interface in Step 2.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>Router(config-if)# pvc vpi/vci</code></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>Step 6</td>
<td>`Router(config-if)# xconnect peer-router-id vcid {encapsulation mpls</td>
<td>pseudowire-class name}`</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>Router(config-if)# end</code></td>
<td>Exits configuration mode.</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
- Configuring an IMA Interface
- Configuring the ATM over MPLS Pseudowire Interface

### Configuring the Controller

Follow these steps to configure the controller.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config)# card type e1 0 0</td>
</tr>
<tr>
<td></td>
<td>Configures IMA on an E1 or T1 interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config)# controller E1 0/4</td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)#</td>
</tr>
<tr>
<td></td>
<td>Specifies the controller interface on which you want to enable IMA.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Router(config-controller)# clock source internal</td>
</tr>
<tr>
<td></td>
<td>Sets the clock source to internal.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Router(config-controller)# ima-group 0 scrambling-payload</td>
</tr>
<tr>
<td></td>
<td>If you want to configure an ATM IMA backhaul, use the <strong>ima-group</strong> command to assign the interface to an IMA group. For a T1 connection, use the <strong>no-scrambling-payload</strong> to disable ATM-IMA cell payload scrambling; for an E1 connection, use the <strong>scrambling-payload</strong> parameter to enable ATM-IMA cell payload scrambling.</td>
</tr>
<tr>
<td></td>
<td>The example assigns the interface to IMA group 0 and enables payload scrambling.</td>
</tr>
<tr>
<td>Step 7</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# exit</td>
</tr>
<tr>
<td></td>
<td>Router#</td>
</tr>
<tr>
<td></td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>
Configuring an IMA Interface

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

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

<table>
<thead>
<tr>
<th>Command</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> Router(config-controller)# interface ATM slot/IMA group-number</td>
<td>Specifies the slot location and port of IMA interface group. The syntax is as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-controller)# interface atm0/ima0 Router(config-if)#</td>
<td>• slot—The slot location of the interface module.</td>
</tr>
<tr>
<td></td>
<td>• group-number—The group number of the IMA group.</td>
</tr>
<tr>
<td></td>
<td>The example specifies the slot number as 0 and the group number as 0.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Router(config-if)# no ip address</td>
<td>Disables the IP address configuration for the physical layer interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Router(config-if)# atm bandwidth dynamic</td>
<td>Specifies the ATM bandwidth as dynamic.</td>
</tr>
</tbody>
</table>
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 encodings. Complete these steps to map a single PVC to an ATM over MPLS pseudowire.

**Note**
Release 15.1(1)MR does not support mapping multiple VCCs to a pseudowire.

<table>
<thead>
<tr>
<th>Command</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></td>
<td></td>
</tr>
<tr>
<td>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></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface atm0/ima0</td>
<td>Configures the ATM IMA interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> pvc 0/40 l2transport</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><strong>Step 5</strong> encapsulation aal0</td>
<td>Defines the encapsulation type for the PVC. The default encapsulation type for the PVC is AAL5.</td>
</tr>
<tr>
<td><strong>Step 6</strong> xconnect 1.1.1.1 40 encapsulation mpls</td>
<td>Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding PVC 40 to the remote peer 1.1.1.1.</td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>

**Command Purpose**

**Step 1**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2**

```
Router# configure terminal
```

Enters global configuration mode.

**Step 3**

```
Router(config)# interface atm0/ima0
```

Configures the ATM IMA interface.

**Step 4**

```
Router(config-if-atm)# pvc 0/40 l2transport
```

Defines a PVC. Use the `l2transport` keyword to configure the PVC as a layer 2 virtual circuit.

**Step 5**

```
Router(config-if-atm-l2trans-pvc)# encapsulation aal0
```

Defines the encapsulation type for the PVC. The default encapsulation type for the PVC is AAL5.

**Step 6**

```
Router(config-if-atm-l2trans-pvc)# xconnect 1.1.1.1 40 encapsulation mpls
```

Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding PVC 40 to the remote peer 1.1.1.1.

**Step 7**

```
Router(config-if-atm-l2trans-pvc-xconnect)# end
```

Exits configuration mode.
Chapter 12 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config)# interface atm0/ima0.x multipoint</td>
</tr>
<tr>
<td></td>
<td>Configures the ATM IMA multipoint interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config-subif)# xconnect 1.1.1.1 40 encapsulation mpls</td>
</tr>
<tr>
<td></td>
<td>Creates a pseudowire on an ATM IMA interface. This example creates a pseudowire to the remote peer 1.1.1.1.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Router(config-subif-xconn)# pvc 0/40 l2transport</td>
</tr>
<tr>
<td></td>
<td>Defines the first PVC 0/40 and maps it under the pseudowire created in Step 4. Use the l2transport keyword to configure the PVC as a layer 2 virtual circuit.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Router(config-if-atm-l2trans-pvc)# pvc 0/41 l2transport</td>
</tr>
<tr>
<td></td>
<td>Defines the second PVC 0/41 and maps it under the pseudowire created in Step 4. Use the l2transport keyword to configure the PVC as a layer 2 virtual circuit.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Router (config-if-atm-l2trans-pvc)# end</td>
</tr>
<tr>
<td></td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>

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

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.
### Configuring an ATM over MPLS Pseudowire

#### 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.

<table>
<thead>
<tr>
<th>Command</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>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config)# interface atm 0/ima 0</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config-if-atm)# atm pvp 10 l2transport</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Router(config-if-atm-l2trans-pvp)# xconnect 30.30.30.2 305 encapsulation mpls</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Router(config-if-atm-l2trans-pvp-xconn)# end</td>
</tr>
</tbody>
</table>

#### Note
You must use the AAL5 encapsulation for this transport type.
## Configuring an ATM over MPLS Pseudowire

A port mode pseudowire allows you to map an entire ATM interface to a single pseudowire connection. Follow these steps to configure a port mode pseudowire:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| **Example:**
  Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**
  Router# configure terminal | |
| **Step 3**
  Router(config)# interface atm 0/ima0 | Configures the ATM interface. |
| **Step 4**
  Router(config-if)# xconnect 25.25.25.25 2000 encapsulation mpls | Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 200 to the remote peer 25.25.25.25. |
| **Step 5** exit | Exits configuration mode. |
| **Example:**
  Router(config)# exit
  Router# | |
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config)# int atm1/0</td>
</tr>
<tr>
<td>Configures the ATM interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config)# int atm1/0</td>
</tr>
<tr>
<td>Router(config-if)# atm mcpt-timers 1000 2000 3000</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Router(config)# pvc 0/11 12transport</td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)# encapsulation aal0</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)# cell-packing 20 mcpt-timer 3</td>
<td></td>
</tr>
<tr>
<td>Specifies the maximum number of cells in PW cell pack and the cell packing timer that the Cisco ASR 903 Series Router uses. This example specifies 20 cells per pack and the third MCPT timer.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-atm-l2trans-pvc)# end</td>
</tr>
<tr>
<td>Router#</td>
<td></td>
</tr>
<tr>
<td>Exits the configuration mode.</td>
<td></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 Cisco ASR 903 Series Router supports EoMPLS pseudowires on EVC interfaces.

For more information about Ethernet over MPLS Pseudowires, see Transportation of Service Using Ethernet over MPLS, page 12-5. For more information about how to configure MPLS, see the Cisco IOS XE 3S Configuration Guides. For more information about configuring Ethernet Virtual Connections (EVCs), see Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router.
Follow these steps to configure an Ethernet over MPLS Pseudowire on the Cisco ASR 903 Series Router.

<table>
<thead>
<tr>
<th>Command</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></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the port on which to create the pseudowire and enters interface configuration mode. Valid interfaces are physical Ethernet ports.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Step 4 service instance number ethernet</td>
<td>Configure an EFP (service instance) and enter service instance configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>Step 5 encapsulation [default</td>
<td>dot1q</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 12      Configuring Pseudowire

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 12-3 shows an example of pseudowire redundancy.

**Figure 12-3 Pseudowire Redundancy**

---

**Command**

**Step 6**

xconnect peer-ip-address vc-id
{encapsulation [12tpv3 [manual] | mpls [manual]] | pw-class pw-class-name}[pw-class pw-class-name][sequencing [transmit | receive | both]]

**Purpose**

Binds the Ethernet port interface to an attachment circuit to create a pseudowire. This example uses virtual circuit (VC) 101 to uniquely identify the PW. Ensure that the remote VLAN is configured with the same VC.

**Note**

When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as ip route 10.30.30.2 255.255.255.255 10.2.3.4.

**Step 7**

exit

**Example:**

Router (config-if-srv)# xconnect 10.1.1.2 101 encapsulation mpls

**Example:**

Router (config)# exit

Router#

**Command Purpose**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>xconnect peer-ip-address vc-id</td>
<td>Binds the Ethernet port interface to an attachment circuit to create a pseudowire. This example uses virtual circuit (VC) 101 to uniquely identify the PW. Ensure that the remote VLAN is configured with the same VC.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>

---

**Note**

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</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>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 pseudowire-class [pw-class-name]</td>
<td>Specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# pseudowire-class mpls</td>
<td></td>
</tr>
<tr>
<td>Step 4 encapsulation mpls</td>
<td>Specifies MPLS encapsulation.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-pw-class)#</td>
<td></td>
</tr>
<tr>
<td>encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td>Step 5 interface serial slot/subslot/port</td>
<td>Enters configuration mode for the serial interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface serial0/0</td>
<td></td>
</tr>
<tr>
<td>Step 6 Router(config)# backup delay enable-delay (disable-delay</td>
<td>Configures the backup delay parameters.</td>
</tr>
<tr>
<td>never)</td>
<td>Where:</td>
</tr>
<tr>
<td></td>
<td>• enable-delay—Time before the backup PW takes over for the primary PW.</td>
</tr>
<tr>
<td></td>
<td>• disable-delay—Time before the restored primary PW takes over for the backup PW.</td>
</tr>
<tr>
<td></td>
<td>• never—Disables switching from the backup PW to the primary PW.</td>
</tr>
<tr>
<td>Step 7 Router(config-if)# xconnect 1.1.1.2 101 encapsulation mpls</td>
<td>Binds the Ethernet port interface to an attachment circuit to create a pseudowire.</td>
</tr>
<tr>
<td>Step 8 Router(config)# backup peer peer-router-ip-address vcid [pw-class pw-class name]</td>
<td>Defines the address and VC of the backup peer.</td>
</tr>
<tr>
<td>Step 9 exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Router#</td>
<td></td>
</tr>
</tbody>
</table>
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 ckt(s)
  | Output modifiers
  
  Router# show cem circuit
  CEM Int.       ID   Line    Admin   Circuit       AC
  ----------------------------------------------
  CEM0/1/0       1    UP      UP    ACTIVE       --/--
  CEM0/1/0       2    UP      UP    ACTIVE       --/--
  CEM0/1/0       3    UP      UP    ACTIVE       --/--
  CEM0/1/0       4    UP      UP    ACTIVE       --/--
  CEM0/1/0       5    UP      UP    ACTIVE       --/--
  
  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 RatePacket Loss
  Signalling: No CAS
  Ingress Pkt: 25929 Dropped: 0
  Egress Pkt: 0 Dropped: 0
  CEM Counter Details
  Input Errors: 0 Output Errors: 0
  Pkts Missing: 25927 Pkts Reordered: 0
  Misorder Drops: 0 JitterBuf Underrun: 1
  Error Sec: 26 Severly Errored Sec: 26
  Unavailable Sec: 5 Failure Counts: 1
  Pkts Malformed: 0

- **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 RatePacket Loss
  Signalling: No CAS
  Ingress Pkt: 25929 Dropped: 0
  Egress Pkt: 0 Dropped: 0
  CEM Counter Details
  Input Errors: 0 Output Errors: 0
  Pkts Missing: 25927 Pkts Reordered: 0
  Misorder Drops: 0 JitterBuf Underrun: 1
  Error Sec: 26 Severly Errored Sec: 26
  Unavailable Sec: 5 Failure Counts: 1
  Pkts Malformed: 0
  
  Router# show cem circuit summary
  CEM Int. Total Active Inactive
  -------------------------------
  CEM0/1/0 5 5 0
  
  show running configuration—The **show running configuration** command shows detail on each CEM group.
Configuration Examples

The following sections contain sample pseudowire configurations.

- Example: CEM Configuration, page 12-28
- Example: ATM IMA Configuration, page 12-28
- Example: ATM over MPLS, page 12-29
- Example: Ethernet over MPLS, page 12-36

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 Chapter 12, “Configuring Pseudowire.”

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: 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 Chapter 12, “Configuring Pseudowire.”

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, page 12-29
- Cell Relay Configuration Examples, page 12-33

Cell Packing Configuration Examples

The following sections contain sample ATM over MPLS configuration using Cell Relay:

- VC Mode, page 12-29
- VP Mode, page 12-31

VC Mode

CE 1 Configuration

```plaintext
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 50.1.1.1
```

CE 2 Configuration

```plaintext
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 50.1.1.2
```
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
configuration examples

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 l2transport
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 l2transport
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, page 12-33
- VP Mode, page 12-35

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**

```conf
! 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 12transport
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**

```conf
! 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 12transport
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**

```plaintext
! 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**

```plaintext
! 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**

```plaintext
interface Loopback0
ip address 192.168.37.3 255.255.255.255
!
interface ATM0/0/0
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 12transport
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 GigabitEthernet0/0/4
!

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
!

Quality of Service Configuration Guidelines

This document outlines Quality of Service features and limitations available on the Cisco ASR 903 Series Router and contains the following sections:

New and Changed Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
</table>
• Egress Policing Limitations, page 13-27 |
| • Support for police and set commands in same class-map. | Police and set can be configured on same egress policy class-map. | | |
| • Support for QoS policies on layer 3 Etherchannel interfaces. | Ingress and Egress QoS policies are supported on etherchannel. | Cisco IOS XE Release 3.9 | • Etherchannel QoS Limitations, page 13-5 |
| • Support for QoS matching on Ethernet service instances | Match EFP is supported on service instances. | Cisco IOS XE Release 3.8 | • Classifying Traffic Using Match EFP Service Instance Feature, page 13-18 |
Understanding Quality of Service

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including ATM, Ethernet and 802.1 networks, SONET, and IP-routed networks. In particular, QoS features provide improved and more predictable network service by implementing the following services:

- Supporting guaranteed bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

For more information about Quality of Service, see http://www.cisco.com/en/US/products/ps11610/products_installation_and_configuration_guides_list.html
Configuring Quality of Service

This document provides details on the platform-dependent implementation of QoS on the Cisco ASR 903 Series Router. For information about how to understand and configure QoS features, see http://www.cisco.com/en/US/products/ps11610/products_installation_and_configuration_guides_list.html

QoS Support Overview

This table provides an overview of QoS feature support on the Cisco ASR 903 Series Router. For more detail about the support for each feature, see QoS Limitations and Guidelines, page 13-4.

Table 13-2 QoS Feature Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Main</th>
<th>Service Instance</th>
<th>Trunk EFP</th>
<th>Port-Channel</th>
<th>Member Link</th>
<th>MLPPP Bundle</th>
<th>Serial Ifc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic policy modification</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>EFP QoS Support</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic policy modification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5.1</td>
<td>3.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Egress</td>
<td>3.6</td>
<td>3.6</td>
<td>3.5.1</td>
<td>3.6</td>
<td>3.5</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Match any</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Marking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5.1</td>
<td>3.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Egress</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Policing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5.1</td>
<td>3.5</td>
<td>3.5</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Egress</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Priority policing</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Shaping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Shaping</td>
<td>3.6.1</td>
<td>3.6.1</td>
<td>3.6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Congestion Avoidance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Multiple Priority Queues</td>
<td>3.7</td>
<td>3.7</td>
<td>3.7</td>
<td>3.7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Congestion Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strict Priority</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5.1</td>
<td>3.5</td>
<td>3.5</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Scheduling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5.1</td>
<td>3.5</td>
<td>3.5</td>
<td>3.7.1</td>
<td></td>
</tr>
<tr>
<td>Egress</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5.1</td>
<td>3.5</td>
<td>3.5</td>
<td>3.7.1</td>
<td></td>
</tr>
</tbody>
</table>
QoS Limitations and Guidelines

- Global QoS Limitations, page 13-4
- Classification, page 13-14
- Marking, page 13-20
- Policing, page 13-24
- Shaping, page 13-29
- Congestion Management, page 13-30
- Congestion Avoidance, page 13-33
- Scheduling, page 13-38
- Scheduling, page 13-38

Global QoS Limitations

The following limitations apply to multiple QoS features for the Cisco ASR 903 Series Router:

- When EVCs under a physical interface have a QoS policy attached, the following limitations apply:
  - The port-level policy is limited to the class-default class
  - Only the `shape` command is supported in the port-level policy
- The Cisco ASR 903 Series Router supports up to 64 unique QoS classification service instances in a given bridge domain. QoS service instances refer to ports, VLAN classes, EFPs associated with a QoS classification policy.
- Modification of class-map definitions while applied to an interface or Ethernet Flow Point is not supported.
- Policy validation—Some QoS policy configurations are not validated until you apply the policy-map to an interface or Ethernet Flow Point. If a QoS configuration is invalid, the router rejects the configuration when you apply it to an interface. In some cases, a QoS configuration may be rejected due to hardware resource exhaustion or limitations. If you receive such an error message, detach the policy and adjust your QoS configuration.
- The `match-all` keyword is supported only for QinQ classification.
- SAToP and CESoPSN pseudowire traffic has a default MPLS Exp priority setting of 5 (high).
- QoS is supported on POS interfaces on optical interface module.
- Three-level QoS policies are not supported on the OC-3/OC-12 serial, MLPPP, and PoS interfaces. You can only apply QoS policies on two levels on these interfaces.
QoS Limitations and Guidelines

- QoS does not account for CRC values on an interface and assumes that the value is 2 bytes. CRC differences can cause accuracy issues for 2 to 3% of the 128-byte traffic.
- The Cisco ASR 903 router supports a maximum of 128 internal and reserved labels that represent PHB (cos/dscp/exp/prec) values on a QoS policy. A label exhaustion message is displayed if a policy exceeds the maximum number of labels.

QoS Features Using MQC Limitations

Table 13-3 lists the QoS MQC scaling limitations on router per release.

<table>
<thead>
<tr>
<th>Supported on Cisco ASR 903&lt;sup&gt;1&lt;/sup&gt;</th>
<th>Cisco IOS XE 3.5S</th>
<th>Cisco IOS XE 3.6S</th>
<th>Cisco IOS XE 3.7S</th>
<th>Cisco IOS XE 3.8S</th>
<th>Cisco IOS XE 3.9S</th>
<th>Cisco IOS XE 3.10S</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of unique policy-maps</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No. of unique class-maps</td>
<td>4096</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No. of classes per policy-map</td>
<td>512</td>
<td></td>
<td></td>
<td></td>
<td>4096</td>
<td></td>
</tr>
<tr>
<td>No. of filters per class-map</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. For releases which are not listed, refer to the most recent previous release limit.

Etherchannel QoS Limitations

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links. Release 3.9 introduces support for QoS policies on layer 3 Etherchannel interfaces.

The following features are supported on either etherchannels or member links, ingress and egress direction:
- Marking
- Policing

Note: You cannot configure these features on an etherchannel interface and a member link at the same time.

The following features are supported only on member links:
- shaping
- bandwidth
- priority
- QL/WRED

Ingress QoS

Restrictions for Ingress QoS in the Cisco IOS Release 3.9 and later:
- EC main interface
  - Only policing and marking are supported.
  - A class-map can have any type of filter, including the match vlan and match service instance commands.
Chapter 13      Quality of Service Configuration Guidelines

QoS Limitations and Guidelines

- EC EVC/TEFP
  - Only policing and marking are supported.
  - Match service instance is not supported.
- Member links
  - Only policing and marking are supported.
  - Policy-map on a member link is not supported with EVC configured at the port-channel level.
- Policy-map application is allowed only on the EC main interface, EC member link, or EC EVC.
- Ingress TCAM entries are used even if no member links exist for a policy on the EC main interface and EC EVCs.

Egress QoS

Restrictions for Egress QoS in the Cisco IOS XE Release 3.9 and later:
- EC main interface
  - Classification statistics for the policy-map on a port-channel main interface are not supported as no queues are allocated for a port-channel main interface.
  - Policing and marking actions are only allowed in the policy-map on a port-channel main interface.
  - Queuing actions are not supported.
  - Egress TCAM entries are used even in the absence of member links.
- EC EVC/TEFP
  - Classification statistics for the policy-map on port-channel EVC/TEFP are not supported as no queues are allocated for port-channel EVC/TEFP.
  - Policing and marking actions are only allowed in the policy-map on port-channel EVC/TEFP.
  - Queuing actions are not supported.
  - Egress TCAM entries are used even if there are no member links present.
- EC Member links
  - For egress match service-instance policy-map on EC member links, the same policy must be present on all other EC member links.
  - Match service-instance policy-map is replicated automatically for all the member links when the first policy is applied on any of the member links.
  - For non-match service-instance policy-map, the same policy-map can be applied for all member-links.
  - Dynamic modification of match service-instance policy-map actions is not allowed.
  - Deleting a global match service instance policy-map is not allowed if it applied to the member links.
  - Policing, marking and queuing action are supported on port-channel member links.
  - The running configuration displays the first member link on the first policy applied in a service-policy configuration.
  - The show policy-map interface brief command only displays the policy-map applied on the running configuration.
– Applying a same policy again on other member links where a policy-map was already applied will not display any error. A differently named policy if applied again will display an error.

– For match service instance policy-map on egress member links, the policy-map statistics information is reset, when a member link is added or deleted from a port-channel either by configuration or by LACP port-bundling/unbundling action.

– There is no difference in behavior for non-match service instance policies on the member links. They continue to work in the legacy mode. There is no conservation of TCAM entries in this mode, even if the same policy is applied on all member links.

– Policy-map application is allowed only on either EC main interface, or EC member link, or EC EVC.

### Routed Port-Channel

#### Routed Port-channel Interface

The following features are supported for the ingress policy-map on a routed port-channel interface:

- Marking
- Policing
- Conditional marking
- Marking and policing
- Classification criteria is prec, dscp or ip acl.

This is an example:

```plaintext
policy-map routed_pc_ingress
  class prec1
  set prec 2
  class prec2
  police cir 100m
  class prec3
  police cir 150m conform-action set-prec-transmit 4 exceed-action drop
  class prec4
  police cir 200m
  set prec 0
! end
```

The following features are supported for egress policy-map on routed port-channel interface:

- Marking
- Policing
- Classification criteria is prec or dscp.

This is an example:

```plaintext
policy-map pc_egress
  class dscp0
  set dscp 16
  class dscp48
  police cir 1m
! end
```
Member-links on Routed Port-channel Interface

The following features are supported for ingress policy-map on member links on the routed port-channel interface:

- Marking
- Policing
- Conditional marking
- marking and policing
- Classification criteria is prec, dscp or ip acl.

The following features are supported for egress policy-map on member links on the routed port-channel interface:

- Shaping
- Queue-limit
- Bandwidth (kbps, percent)
- Bandwidth remaining (ratio, percent)
- WRED
- Port Shaper
- Low Latency Queue (LLQ or priority queue)

This is an example:

```plaintext
policy-map mem_link_egress
class qos-group0
bandwidth percent 90
class qos-group67
police cir 1m
priority
class class-default
shape average 64k
!
end
```

Port-channel with EFP

The following features are supported for ingress policy-map on port-channel on EFP:

- Marking
- Policing
- Conditional marking
- marking and policing
- The classification criteria is VLAN or EFP, Cos in child.

This is an example:

```plaintext
policy-map cos_child
class cos0
set cos1
!
policy-map efp_pc_ingress
class vlan100
police cir 10m
service-policy cos_child
!```
The following features are supported for egress policy-map on port-channel on EFP:

- Marking
- Policing
- Conditional marking
- marking and policing
- The classification criteria is VLAN or EFP, Cos in child

This is an example:

```
policy-map cos_child
  class cos0
  set cos1
!
policy-map efp_pc_ingress
  class vlan100
  police cir 10ms
  service-policy cos_child
!
end
```

**EFP of Port-channel with EFP Configuration**

- The following features are supported for ingress and egress policy-map on EFP of port-channel on EFP:
  - Marking
  - Policing
  - Conditional marking
  - marking and policing
  - The classification criteria is VLAN or EFP, Cos in child.

**Note**

Match EFP is cannot be configured.

**Member Links of Port-channel with EFP Configuration**

- The following features are supported for ingress and egress policy-map on member links of port-channel on EFP:
  - Marking
  - Policing
  - Conditional marking
  - marking and policing
  - The classification criteria is VLAN or EFP, Match VLAN and Cos in child.
Restrictions for Hierarchical Policies

The Cisco ASR 903 Router supports hierarchical QoS policies with up to three levels, allowing for a high degree of granularity in traffic management.

There are limitations on the supported classification criteria at each level in the policy-map hierarchy. The following limitations apply when configuring hierarchical policy-map classification:

- The topmost policy-map in a three-level hierarchy only supports classification using class-default.

Sample Hierarchical Policy Designs

The following are examples of supported policy-map configurations:

- Three-Level Policy—You can only apply a three-level policy to a physical port on the router. A three-level policy consists of:
  - Topmost policy: class-default
  - Middle policy: match vlan
  - Lowest policy: match qos-group/match prec/match cos/match dscp

The following sample policy uses a flat class-default policy on the port and VLAN policies on EFP interfaces to unique QoS behavior to each EFP.

Sample Policy

```
Policy-map port-shaper
Class class-default
Shape average percent 70
Service-policy Vlan_set

Policy-map Vlan_set
Class vlan100
Bandwidth percent 20
Shape average 200m
Service-policy child1
Class vlan200_300
Bandwidth percent 75
Service-policy child2

Policy-map child1
Class prec2
Shape average percent 40

Policy-map child2
Class prec4
Police cir percent 50
```

- Two-Level Policy
  - Topmost policy: match vlan
  - Lowest policy: match qos-group/match prec/match cos/match dscp

- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match vlan

- Two-Level Policy
  - Topmost policy: class-default
Chapter 13  Quality of Service Configuration Guidelines

QoS Limitations and Guidelines

Chapter 13  Quality of Service Configuration Guidelines

QoS Limitations and Guidelines

– Lowest policy: match mpls experimental topmost
– Flat policy: match ip dscp
– Flat policy: match vlan inner
– Flat policy: class-default

Ingress and Egress Hierarchical Policing

In releases before Cisco IOS XE Release 3.9, policing was supported only at one level in the ingress and egress policy. It was only at the PHB or class level.

Effective with Cisco IOS XE Release 3.9, policing is supported at two levels of the policy-map.

– Ingress policing
  – Port and EFP level
  – EFP and Class level
  – Port and Class level
– Egress policing
  – EFP and Class level
  – Port and Class level

Note  Egress hierarchical policing is supported on two levels but one of the levels must be Class level.

If an Ingress hierarchical policy is configured on the interface, the show Ethernet service instance interface command does not display the service instance statistics.

The class-level in an Egress hierarchical policy is configured internally as shaper.

MPLS VPN QoS Mapping

Table 13-4  summarizes the default MPLS mappings for the Cisco ASR 903 Series Router.

Table 13-4  Default MPLS QoS Mapping

<table>
<thead>
<tr>
<th>Feature</th>
<th>Imposition</th>
<th>Disposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3VPN, MPLS</td>
<td>IP Prec bit copied to MPLS Exp bit.</td>
<td>IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.</td>
</tr>
<tr>
<td>L2VPN (EoMPLS, VPLS)</td>
<td>MPLS Exp bit is set to 0</td>
<td>IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.</td>
</tr>
<tr>
<td>MPLS-TP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CESoPN</td>
<td>MPLS Exp bit is set to 5</td>
<td>IP Prec bit is unchanged.</td>
</tr>
<tr>
<td>SAToP</td>
<td>MPLS Exp bit is set to 5</td>
<td>IP Prec bit is unchanged.</td>
</tr>
<tr>
<td>6VPE, 6PE</td>
<td>Prec bit value is copied to the MPLS Exp bit</td>
<td>IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.</td>
</tr>
</tbody>
</table>
QoS Policer and Shaper Calculation

Table 13-5 summarizes the packet accounting information used to make policer and shaper calculations on the Cisco ASR 903 Series Router.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Direction</th>
<th>Traffic Type</th>
<th>Values Counted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policing</td>
<td>Ingress</td>
<td>IPv4/L3VPN</td>
<td>L2 overhead, VLAN tag, CRC</td>
</tr>
<tr>
<td>Shaping</td>
<td>Egress</td>
<td>IPv4/L3VPN</td>
<td>L2 Ethernet overhead, VLAN tag, CRC, preamble, IPG</td>
</tr>
<tr>
<td>Policing</td>
<td>Egress</td>
<td>IPv4/L3VPN</td>
<td>Layer 2 Ethernet overhead, VLAN</td>
</tr>
<tr>
<td>Policing</td>
<td>Ingress</td>
<td>L2VPN</td>
<td>Layer 2 Ethernet overhead, VLAN tag, CRC</td>
</tr>
<tr>
<td>Shaping</td>
<td>Egress</td>
<td>L2VPN</td>
<td>Layer 2 Ethernet overhead, VLAN tag, CRC, preamble, IPG</td>
</tr>
<tr>
<td>Policing</td>
<td>Egress</td>
<td>L2VPN</td>
<td>Layer 3 payload (without CRC)</td>
</tr>
</tbody>
</table>

The following considerations also apply when understanding QoS policer and shaper calculations:

- Egress shaping is applied at layer 1.
- Ingress packet length accounting is performed at egress.
- Egress shaping and policing do not account for newly pushed VLAN tags and MPLS labels.
- If two policers are configured at egress, the statistics on the child PHB or PQ level are not displayed.

Implementing MPLS Diffserv Tunneling Modes

The MPLS specification defines three Diffserv operation modes:

- Uniform—There is only one Diffserv marking that is relevant for a packet when traversing the MPLS network.
- Pipe—The network uses two markings for traffic: the original marking value, which is used once the packets leave the MPLS network, and a separate marking value that is used while the traffic crosses intermediate nodes on the LSP span. The second marking value is dropped when traffic exits the MPLS network.
- Short-Pipe—the egress LSR uses the original packet marking instead of using the marking used by the intermediate LSRs.

The following sections describe how to implement these modes on the Cisco ASR 903 Series Router using QoS policies.

Implementing Uniform Mode

Use the following guidelines to implement uniform mode on the Cisco ASR 903 Series Router:

Imposition

To copy the diffserv value to the MPLS Exp bit, create a QoS configuration as follows:
• Option 1
  – Classify based on Prec bit or DSCP bit at ingress.
  – Set the qos-group.
  – Classify on qos-group.
  – Set the MPLS exp value.

• Option 2
  – Classify based on Prec bit or DSCP bit at ingress.
  – Set the mpls Exp bit at imposition.

Tag-to-tag Transfer
To ensure that outer tag values are copied to inner tags, explicitly mark the outer Exp value on the inner Exp bit.

Disposition
To copy the MPLS Exp bit to the diffserv/IP prec bit, create a QoS configuration as follows:
• Classify based on MPLS Exp bit on the ingress interface.
• Set the qos-group value.
• Classify based on qos-group on the egress interface.
• Mark the IP prec or DSCP bit.

Implementing Pipe Mode
Use the following guidelines to implement pipe mode on the Cisco ASR 903 Series Router:

Imposition
To set the MPLS Exp bit by policy, create a QoS configuration as follows:
• Option 1
  – Set the qos-group on the egress interface.
  – Classify based on qos-group on the egress interface.
  – Set the MPLS Exp value.

• Option 2
  – Apply the set mpls exp imposition command at ingress.

Disposition
To preserve the original IP Prec or diffserv value so that egress queuing is based on MPLS exp value, create a QoS configuration as follows:
• Classify on MPLS Exp value on the ingress interface.
• Set the qos-group on the egress interface.
• Classify based on qos-group value on the egress interface.
Implementing Short-Pipe Mode

Use the following guidelines to implement short-pipe mode on the Cisco ASR 903 Series Router:

**Disposition**

To preserve the original IP Prec or diffserv value so that egress queuing is based on MPLS Prec or diffserv value, create a QoS configuration as follows:

- Classify based on IP prec or DSCP value on the egress interface.
- Mark the IP prec or DSCP bit.

**Classification**

Classifying network traffic allows you to organize packets into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic (used in conjunction with marking network traffic) is the foundation for enabling many quality of service (QoS) features on your network.

- Ingress Classification Limitations, page 13-16
- Egress Classification Limitations, page 13-16
- Additional Classification Limitations, page 13-16
- Classifying Traffic using an Access Control List, page 13-16
- Configuring Multiple match Statements, page 13-18
- Classifying Traffic Using Match EFP Service Instance Feature, page 13-18

Table 13-5 summarizes the QoS Classification limitations for the Cisco ASR 903 Series Router.

### Table 13-6  QoS Classification Limitations

<table>
<thead>
<tr>
<th>Match</th>
<th>Main Layer 3 Interface</th>
<th>EFP Interface</th>
<th>Trunk EFP</th>
<th>L3 Ether Channel</th>
<th>L2 Port Channel</th>
<th>L3 Port Channel Member</th>
<th>L2 Port Channel Member</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>MLPPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
</tr>
<tr>
<td>Multiple match statements</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>access-group</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>all</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>any</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>class-map</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>cos</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>cos inner</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>destination-address</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### Table 13-6  QoS Classification Limitations (continued)

<table>
<thead>
<tr>
<th>Match</th>
<th>Main Layer 3 Interface</th>
<th>EFP Interface</th>
<th>Trunk EFP</th>
<th>L3 Etherchannel</th>
<th>L2 Port Channel</th>
<th>L3 Port Channel Member</th>
<th>L2 Port Channel Member</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>MLPPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>discard-class</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>dscp (IPv4)</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>dscp (IPv6)</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>flow pdp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>frde</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>frdci</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ip dscp</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>ip precedence (IPv4)</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>ip precedence (IPv6)</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>ip rtp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mpls experimental</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>mpls experimental topmost</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>not</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>packet length</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>precedence (IPv4)</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>precedence (IPv6)</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>protocol</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>qos-group</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>service instance ethernet</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>source-address</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vlan</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
<tr>
<td>vlan inner</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.7.1</td>
</tr>
</tbody>
</table>
Ingress Classification Limitations

The following limitations apply to QoS classification on the Cisco ASR 903 Series Router:

- If you configure egress classification for a class of traffic affected by an input policy-map, you must use the same QoS criteria on the ingress and egress policy-maps.

Egress Classification Limitations

- When applying a QoS policy to a link aggregation group (LAG) bundle, you must assign the policy to a physical link within the bundle; you cannot apply the policy to the LAG bundle or the port channel interface associated with the bundle.
- MPLS Pipe Mode Limitations—When you configure pipe mode for Time to Live (TTL), the router enables pipe mode for QoS as well. When pipe mode is enabled, you cannot enable egress classification based on the header on an egress interface. For example, you cannot classify based on egress DSCP value for MPLS IP packets when the router is in pipe mode.
- If you configure egress classification for a class of traffic affected by an input policy-map, you must use the same QoS criteria on the ingress and egress policy-maps.

Classifying Traffic on MLPPP Interfaces

Release 3.7(1) introduces support for egress QoS on MLPPP interfaces. The Cisco ASR 903 Series Router supports the following `match` commands in a QoS class-map applied to an egress MLPPP interface.

- `match discard-class`
- `match dscp`
- `match ip dscp`
- `match ip precedence`
- `match precedence`
- `match qos-group`

Additional Classification Limitations

The following additional marking usage guidelines apply in Release 3.9:

- The topmost policy-map in a three-level hierarchy only supports classification using class-default.
- If you configure egress classification for a class of traffic affected by an input policy-map, you must use the same QoS criteria on the ingress and egress policy-maps.

Classifying Traffic using an Access Control List

You can classify inbound packet based on an IP standard or IP extended access control list (ACL). Follow these steps to classify traffic based on an ACL:

1. Create an access list using the `access-list` or `ip access-list` commands
2. Reference the ACL within a QoS class map using the `match access-group` configuration command
3. Attach the class map to a policy map
Limitations and Usage Guidelines

The following limitations and usage guidelines apply when classifying traffic using an ACL:

- QoS ACLs are supported only for IPv4 traffic
- QoS ACLs are supported only for ingress traffic
- You can use QoS ACLs to classify traffic based on the following criteria:
  - Source and destination host
  - Source and destination subnet
  - TCP source and destination
  - UDP source and destination
- Named and numbered ACLs are supported.
- You can apply QoS ACLs only to the third level class (bottom-most).
- The following range of numbered access lists are supported:
  - 1-99—IP standard access list
  - 100-199—IP extended access list
  - 1300-1999—IP standard access list (expanded range)
  - 2000-2699—IP extended access list (expanded range)
- You must create an ACL before referencing it within a QoS policy.
- Deny statements within an ACL are ignored for the purposes of classification.
- Classifying traffic based on TCP flags using an ACL is not supported.
- Classifying traffic using multiple mutually exclusive ACLs within a match-all class-map is not supported.
- Classifying traffic on a logical/physical level using an ACL is not supported.
- Applying QoS ACLs to MAC addresses is not supported.
- Port matching with the neq keyword is only supported for a single port.
- Matching on multiple port numbers using the eq keyword is supported for up to 8 ports.
- You can only configure 8 port matching operations on a given interface. A given command can consume multiple matching operations if you specify a source and destination port, as shown in the following examples:
  - permit tcp any lt 1000 any—Uses one port matching operation
  - permit tcp any lt 1000 any gt 2000—Uses two port matching operations
  - permit tcp any range 1000 2000 any 400 500—Uses two port matching operations
You can use the following commands to verify your configuration:
  - show platform hardware pp {active | standby} acl label labelindex—Displays information about security ACL labels; the number of available input VMRs reflects the number of available port range operations.
- Only the following combination of matches are currently supported for Ingress policies:
  - Combination A: DSCP, Outer COS, UDP/TCP Source and Destination port number, IP SA/DA
  - Combination B: IP SA/DA, Outer COS, Inner COS, DSCP, MPLS EXP
  - Combination C: MAC DA, Outer COS, Inner COS, DSCP, MPLS Exp
QoS Limitations and Guidelines

Chapter 13  Quality of Service Configuration Guidelines

Note
Policy with match on L4 ACL and MPLS EXP together is currently not supported.


Configuring Multiple match Statements

In IOS XE Release 3.5, the Cisco ASR 903 Series Router supported a single match or match-any command in a given QoS class-map, as shown in the following example:

**IOS XE 3.5 Class Map Example**

```plaintext
class-map match-any my-restrict-class_00
  match ip prec

class-map match-any my-restrict-class_01
  match qos-group 2

class-map match-any my-restrict-class_03
  match cos 3
```

IOS XE Release 3.6 introduces support for multiple match or match-any commands in a given QoS class-map, as shown in the following example:

**IOS XE 3.6 Class Map Example**

```plaintext
class-map match-any my-class
  match ip prec 1
  match qos-group 2
  match cos 3
```

The router treats the statements as a logical OR operation and classifies traffic that matches any match statement in the class map.

Classifying Traffic Using Match EFP Service Instance Feature

Service Provider configurations have various service instances on the PE. QoS policy-maps are applied on these service instances or group of service instances. Cisco IOS XE Release 3.9S introduces the Match EFP Service Instance feature. The benefits of this feature are:

- Identify the various types of service-instances like EFP, Trunk EFPs
- Apply policies on these service instances at the port
- Manage bandwidth and priority across the service instances on the port and across classes within the service instance
- Apply policies on a group of transport service instances such as applying similar policies to a group of EFPs.
Configuring Match Service Instances

Restrictions

- Ethernet service instances configured under the interface can be classified in a class of a policy-map. The class can match on a group or set of match service instance statements.

```plaintext
class-map match-any policeServiceInstance
  match service instance ethernet 100
  match service instance ethernet 200
```

- Ingress and Egress Match service instance are supported.

- **match service instance** and **match PHB per flows classification** are defined at respective levels in the policy hierarchy under the port.

- The number of EFPs supported per group is 256. Only 256 match statements are supported per class.

- Match EFP policy-map can be configured only on the port and **not** under the service instance.

Example

```plaintext
interface GigabitEthernet0/3/4
no ip address
negotiation auto
service-policy output BTS_Total
service instance 10 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
  service instance trunk 20 ethernet
    encapsulation dot1q 20-29
    rewrite ingress tag pop 1 symmetric
    bridge-domain from-encapsulation
!
  service instance 30 ethernet
    encapsulation dot1q 30
    xconnect 192.44.32.21 101 encapsulation mpls

class-map match-any service-instance-group-with-BMG
  match service instance ethernet 10
  match service instance ethernet 20

class-map service-instance-30
  match service instance ethernet 30

class-map service-instance-20
  match service instance ethernet 20

class-map VOICE
  match qos-group 0

class-map SIGNALING
  match qos-group 1

class-map match-any DATA
  match qos-group 2
  match qos-group 4

policy-map child-X
  class VOICE
  priority level 1
```
police cir 20m
class SIGNALING
priority level 2
police cir 30m
class DATA
shape average 90m
random-detect cos-based

policy-map BTS_OUT_Bi
class service-instance-group-with-BMG
shape average 100m
service-policy child-X
class service-instance-30
shape average 200m
service-policy child-X

policy-map BTS_Total
class class-default
shape average 250m
service-policy BTS_OUT_Bi

Marking

QoS marking allows you to set a desired value on network traffic to make it easy for core devices to classify the packet.

- Marking Overview, page 13-22
- Ingress Marking Limitations, page 13-22
- Egress Marking Limitations, page 13-22
- Marking IPv6 Traffic, page 13-23
- Additional Marking Limitations, page 13-23

Table 13-7 summarizes the QoS Marking limitations for the Cisco ASR 903 Series Router.
### Table 13-7  Marking QoS Limitations (continued)

<table>
<thead>
<tr>
<th>Features</th>
<th>Main Layer 3 Interface</th>
<th>EFP Interface</th>
<th>Trunk EFP</th>
<th>L3 Etherchannel</th>
<th>L2 Port Channel</th>
<th>L3 Port Channel Member</th>
<th>L2 Port Channel Member</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>MLPPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
</tr>
<tr>
<td>dscp-transmit</td>
<td>3.5</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ip dscp</td>
<td>3.5</td>
<td>3.6</td>
<td>3.5</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
</tr>
<tr>
<td>ip precedence</td>
<td>3.5</td>
<td>3.6</td>
<td>3.5</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
</tr>
<tr>
<td>mpls experimental imposition</td>
<td>3.5</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
</tr>
<tr>
<td>mpls experimental imposition qos-group</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mpls experimental imposition topmost</td>
<td>3.5</td>
<td>3.6</td>
<td>3.5</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
</tr>
<tr>
<td>precedence</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
</tr>
<tr>
<td>pre-transmit</td>
<td>3.5</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
<td>3.5</td>
<td>3.9</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>qos-group</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
<td>3.5</td>
<td>3.9</td>
<td>3.9</td>
<td>X</td>
<td>3.9</td>
</tr>
</tbody>
</table>
Marking Overview

The Cisco ASR 903 Series Router supports the following parameters with the set command:

- set cos
- set discard-class
- set ip dscp
- set ip precedence
- set mpls experimental imposition (ingress marking)
- set mpls experimental topmost
- set qos-group

CoS Marking Limitations

The following limitations apply when configuring CoS marking:

- set cos—This set action has no effect unless there is a egress push action to add an additional header at egress. The COS value set by this action will be used in the newly added header as a result of the push rewrite. If there are no push rewrite on the packet, the new COS value will have no effect.
- The set cos inner command is not supported.

Ingress Marking Limitations

The following limitations apply to QoS marking on the Cisco ASR 903 Series Router:

- The Cisco ASR 903 Series Router does not support hierarchical marking.
- You can configure marking and policing for any number of classes on any one of the three levels of the policy-map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level. Marking and policing are not supported on the same level of a policy-map.

Egress Marking Limitations

IOS XE Release 3.6 introduces support for egress marking. The following limitations apply when configuring marking on egress interfaces:

- The set cos inner command is not supported.
- The set mpls experimental imposition command is not supported.
- The set mpls experimental topmost command is supported for marking MPLS Exp bits; other commands for marking MPLS Exp bits are not supported.

Marking Traffic on MLPPP Interfaces

Release 3.7(1) introduces support for egress QoS on MLPPP interfaces. The Cisco ASR 903 Series Router supports the following parameters with the set command on egress MLPPP interfaces:

- set ip dscp
- set ip precedence
Marking IPv6 Traffic

The Cisco ASR 903 supports the following commands for marking both IPv4 and IPv6 packets:

- `set dscp`
- `set precedence`

For more information about IPv6 QoS, see:


Additional Marking Limitations

The following additional marking usage guidelines apply in Release 3.9:

- **CoS marking Limitation**— The `set cos` action has no effect unless there is a egress push action to add an additional header at egress. The COS value set by this action will be used in the newly added header as a result of the push rewrite. If there are no push rewrite on the packet, the new COS value will have no effect.

- The Cisco ASR 903 Series Router does not support hierarchical marking.

- You can configure marking and policing for any number of classes on any one of the three levels of the policy-map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level. Marking and policing are not supported on the same level of a policy-map.

- Ingress marking is not supported on Etherchannel interfaces or member links.


- Marking is supported on Etherchannel interfaces and individual member links; however, you cannot configure marking on both interface levels at once.
Policing

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels or class of service (CoS). This section describes the policing limitations and configuration guidelines for the Cisco ASR 903 Series Router.

- **Ingress Policing Limitations, page 13-27**
- **Egress Policing Limitations, page 13-27**

The Cisco ASR 903 Series Router supports the following policing types:

- Single-rate policer with two color marker (1R2C) (color-blind mode)
- Two-rate policer with three color marker (2R3C) (color-blind mode)

Table 13-8 summarizes the QoS policing limitations for the Cisco ASR 903 Series Router.

### Table 13-8  Policing QoS Limitations

<table>
<thead>
<tr>
<th>Features</th>
<th>Main Layer 3 Interface</th>
<th>EFP Interface</th>
<th>Trunk EFP</th>
<th>L3 Etherchannal</th>
<th>L2 Port Channel</th>
<th>L3 Port Channel Member</th>
<th>L2 Port Channel Member</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>MLPPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limiting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>One rate</td>
<td>3.5</td>
<td>3.6</td>
<td>3.5</td>
<td>3.6</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
<td>3.5</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>One rate and two marking</td>
<td>3.5</td>
<td>3.6</td>
<td>3.5</td>
<td>3.6</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
<td>3.5</td>
<td>3.6</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>Two rates and two Marking</td>
<td>3.5</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.9</td>
<td>3.5</td>
<td>X</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>Two rates and three actions</td>
<td>3.5</td>
<td>X</td>
<td>3.5</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.9</td>
<td>3.5</td>
<td>X</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>Color Aware policing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commands</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bandwidth</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
</tr>
<tr>
<td>bandwidth remaining ratio</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
</tr>
<tr>
<td>bandwidth percent</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
</tr>
</tbody>
</table>
### Supported Commands

The Cisco ASR 903 Series Router supports the following policing commands on ingress interfaces:

<table>
<thead>
<tr>
<th>Features</th>
<th>Main Layer 3 Interface</th>
<th>EFP Interface</th>
<th>Trunk EFP</th>
<th>L3 Etherchannel</th>
<th>L2 Port Channel</th>
<th>L3 Port Channel Member</th>
<th>L2 Port Channel Member</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>MLPPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>police (percent)</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
</tr>
<tr>
<td>police (policy map)</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
</tr>
<tr>
<td>police (policy map class)</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
</tr>
<tr>
<td>police (two rates)</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
</tr>
<tr>
<td>priority</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
</tr>
</tbody>
</table>

**Supported actions**

- drop
- set-qos-transmit
- set-cos-transmit
- set-dscp-transmit
- set-prec-transmit
- set-discard-class-transmit
- set-mpls-experimental-topmost-transmit
- set-mpls-experimental-imposition-transmit
- transmit
Chapter 13      Quality of Service Configuration Guidelines

QoS Limitations and Guidelines

- **police (percent)**—**police cir percent** percentage [burst-in-msec] [bc conform-burst-in-msec ms] [be peak-burst-in-msec ms] [pir percent percentage] [conform-action action [exceed-action action [violate-action action]]]
- **police (policy map)**—**police cir bps** [[bc] normal-burst-bytes [maximum-burst-bytes | [be] [burst-bytes]]] [pir bps [be burst-bytes]] [conform-action action [exceed-action action [violate-action action]]]
- **police (two rates)**—**police cir bps** [bc conform-burst] [pir pir] [be peak-burst] [conform-action action [exceed-action action [violate-action action]]]

The Cisco ASR 903 Series Router supports the following policing commands on egress interfaces:

- **bandwidth (policy-map class)**—**bandwidth** [bandwidth-kbps | remaining percent percentage | account {qinq | dot1q} aal5 subscriber-encaps] [burst-bytes]] [pir bps [be burst-bytes]] [conform-action action [exceed-action action [violate-action action]]]
- **priority—priority** {bandwidth-kbps | percent percentage} [burst]

Several restrictions apply when using egress policing; see the Egress Policing Limitations, page 13-27 section for more information.

Supported Actions

The Cisco ASR 903 Series Router supports the following policing actions on ingress interfaces:

- transmit
- drop
- set-qos-transmit
- set-cos-transmit
- set-dscp-transmit
- set-prec-transmit
- set-discard-class-transmit
- set-mpls-experimental-topmost-transmit
- set-mpls-experimental-imposition-transmit

Configuring Percentage Policing

The router calculates percentage policing rates based on the maximum port PIR rate. The PIR rate is determined as follows:

- Default—Port line rate
- Speed command applied—Operational rate
- Port shaping applied to port—Shaped rate
Ingress Policing Limitations

The following limitations apply to QoS policing on the Cisco ASR 903 Series Router:

- If you configure a policer rate or burst-size that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.

- You can configure marking and policing for any number of classes on any one of the three levels of the policy-map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level.

- If you configure marking using the `set` command, you can only configure policing on that level using the transmit and drop command.

- If you configure a policer using a `set` command, you cannot use the `set` command at other levels of the hierarchical policy-map.

Egress Policing Limitations

IOS XE Release 3.6 introduces support for egress policing. The Cisco ASR 903 Series Router supports the `bandwidth` and `bandwidth-remaining` commands on egress interfaces under the following conditions:

- Mixed bandwidth types are not supported in the same policy. For example, you cannot configure a policy containing both the `bandwidth remaining percent` command and `bandwidth remaining ratio` command.

- The `bandwidth` and `bandwidth-remaining` commands are not supported in a class containing the `priority` command. The `bandwidth` and `bandwidth-remaining` commands must be configured on classes of the same level.

- If you want to create a configuration that uses the `bandwidth` or `bandwidth-remaining` commands and the priority command, you must include a `police` statement in the QoS class.

The following is a sample supported configuration:

```
Router# show policy-map
Policy Map PHB
  Class cos1
    police cir 200000 bc 8000
    conform-action transmit
    exceed-action drop
    priority
  Class cos2
    bandwidth 100
    bandwidth remaining percent 40
  Class cos3
    bandwidth 200
    bandwidth remaining percent 50
```

- The `priority` and `police` commands must not be applied to a class containing the `priority` command

- The `priority` and `police` commands must be applied on a single class.

The following is a sample supported configuration:

```
Router# show policy-map
Policy Map PHB
  Class cos1
    police cir 200000 bc 8000
    conform-action transmit
```
QoS Limitations and Guidelines

Chapter 13  Quality of Service Configuration Guidelines

QoS Limitations and Guidelines

- Egress MLPPP interfaces support a single-rate policer with two color marker (1R2C) (color-blind mode) at the LLQ level.

- Policing is supported on Etherchannel interfaces and individual member links; however, you cannot configure marking on both interface levels at once.

- Egress port-level policing is supported with ingress EFP policy on the router.

The following is a sample supported configuration:

```
Policy-map ingress_policy
  Class cos3
    Set cos 5
Policy-map egress policy
  Class cos5
    Shape average 30m

###Ingress
interface GigabitEthernet0/4/0
  no ip address
  negotiation auto
  service instance 100 ethernet
    encapsulation dot1q 100
  service-policy input ingress_policy  >>>> Ingress policy in EFP
  bridge-domain 100

###Egress
interface GigabitEthernet0/4/0
  no ip address
  negotiation auto
  service-policy output egress_policy   >>>>>Egress policy on Port
  service instance 100 ethernet
    encapsulation dot1q 100
  bridge-domain 100
```

- Release 3.7(1) introduces support for QoS features on egress policing on MLPPP interfaces using the `police` command. Egress MLPPP interfaces support a single-rate policer with two color marker (1R2C) (color-blind mode) at the LLQ level.

- **Police** and **Set** in same policy class-map

  Effective 3.10 and later, **police** and **set** commands can be configured together in the egress policy class-map. In prior releases, an error message was displayed when both **police** and **set** commands were configured.

  Sample example displaying the error message:

  ```
  Router(config)#policy-map egress
  Router(config-pmap)#class p1
  Router(config-pmap-c)#police cir 200m
  Router(config-pmap-c-police)#set prec 2
  Qos:Configuration failed - Set and police not allowed in same class p1 of policy egress
  QoS: Configuration failed. Invalid set
  ```
Egress Policing on Non Priority Queue

Starting Cisco IOS XE Release 3.6 and later, policing is supported at the egress on non priority queues.

Sample configuration:

Router#sh policy-map testp
Policy Map testp
Class cos1
  priority
  police cir 20000000 bc 625000
  conform-action transmit
  exceed-action drop
Class cos2
  police cir 20000000 bc 625000
  conform-action transmit
  exceed-action drop
Class cos4
  police cir 50000000 bc 1562500
  conform-action transmit
  exceed-action drop

Shaping

Traffic shaping allows you to control the speed of traffic that is leaving an interface in order to match the flow of traffic to the speed of the receiving interface. Percentage-based policing allows you to configure traffic shaping based on a percentage of the available bandwidth of an interface. Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

This section describes the shaping limitations and configuration guidelines for the Cisco ASR 903 Series Router.

Table 13-9 summarizes the QoS shaping limitations for the Cisco ASR 903 Series Router.; an X indicates support.

Table 13-9 Shaping Limitations by Interface

<table>
<thead>
<tr>
<th>Features</th>
<th>GigE</th>
<th>10 GigE</th>
<th>EFP</th>
<th>Trunk EFP</th>
<th>Port Channel</th>
<th>Memb er Link</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>Serial</th>
<th>MLPPP</th>
<th>ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Egress</td>
<td>Egress</td>
</tr>
<tr>
<td>Class-Based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frame</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shape</td>
<td>adaptive</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>average</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 13  Quality of Service Configuration Guidelines

QoS Limitations and Guidelines

Additional Shaping Limitations

The following additional shaping usage guidelines apply in Release 3.9:

- Policies using shaping are supported only on individual member links of an etherchannel. Applying a shaping policy directly on an etherchannel interface is not supported.

Configuring Egress Shaping on EFP Interfaces

Configuring an EFP port shaper allows you to shape all EFPs on a port using a port policy with a class-default shaper configuration, as in the following partial sample configuration:

```
policy-map port-policy
  class class-default
    shape average percent 50
policy-map efp-policy
  class class-default
    shape average percent 25
  service-policy child-policy
policy-map child-policy
  class phb-class
  <class-map actions>
```

The following configuration guidelines apply when configuring an EFP port shaping policy:

- When the configuration specifies a shaper rate using a percentage, the router calculates the value based on the operational speed of a port. The operational speed of a port can be the line rate of the port or the speed specified by the `speed` command.
- The rates for `bandwidth percent` and `police percent` commands configured under a port-shaper are based on the absolute rate of the port-shaper policy.
- You can combine a port shaper policy (a flat shaper policy with no user-defined classes) with an egress EFP QoS shaping policy.
- Configure the port shaper policy before configuring other egress QoS policies on EFP interfaces; when removing EFP QoS configurations, remove other egress EFP QoS policies before removing the port shaper policy.

Congestion Management

Congestion management features allow you to control congestion by determining the order in which packets are sent out an interface based on priorities assigned to those packets. Congestion management entails the creation of queues, assignment of packets to those queues based on the classification of the packet, and scheduling of the packets in a queue for transmission.

This section describes the classification limitations and configuration guidelines for the Cisco ASR 903 Series Router.

<table>
<thead>
<tr>
<th>Table 13-9 Shaping Limitations by Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigE</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>fecn-adapt</td>
</tr>
<tr>
<td>max-buffers</td>
</tr>
<tr>
<td>peak</td>
</tr>
</tbody>
</table>
Table 13-10 summarizes the QoS congestion management and queuing limitations for the Cisco ASR 903 Series Router.

### Table 13-10  Congestion Management QoS Limitations

<table>
<thead>
<tr>
<th>Features</th>
<th>Main Layer 3 Interface</th>
<th>EFP Interface</th>
<th>Trunk Etherchannel</th>
<th>L2 Port Channel</th>
<th>L3 Port Channel Member</th>
<th>L2 Port Channel Member</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>MLPPP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
</tr>
<tr>
<td>CBWFQ</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
<td>3.8</td>
</tr>
<tr>
<td>D-CBWFQ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP RTP priority</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Frame Relay IP RTP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Frame Relay PVC Interface Priority Queuing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LLQ</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.9</td>
<td>X</td>
<td>3.8</td>
</tr>
<tr>
<td>D-LLQ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LLQ-FR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom queuing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority Queuing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Commands

| bandwidth (kbps)                  | X         | 3.6     | X         | 3.6     | X         | 3.6     | X         | 3.9     | X         | 3.9     | X         | 3.9     | X         | 3.9     | X         | 3.7.1 |
| bandwidth percent                 | X         | 3.6     | X         | 3.6     | X         | 3.6     | X         | 3.9     | X         | 3.9     | X         | 3.9     | X         | 3.9     | X         | 3.7.1 |
| bandwidth remaining percent       | X         | 3.6     | X         | 3.6     | X         | 3.6     | X         | 3.9     | X         | 3.9     | X         | 3.9     | X         | 3.9     | X         | 3.7.1 |
| bandwidth remaining ratio         | X         | 3.6     | X         | 3.6     | X         | 3.6     | X         | 3.9     | X         | 3.9     | X         | 3.9     | X         | 3.9     | X         | 3.7.1 |
| compression header ip             | X         | X       | X         | X       | X         | X       | X         | X       | X         | X       | X         | X       | X         | X       | X         | X         |
| drop                             | X         | X       | X         | X       | X         | X       | X         | X       | X         | X       | X         | X       | X         | X       | X         | X         |
QoS Limitations and Guidelines

Chapter 13  Quality of Service Configuration Guidelines

Table: QoS Limitations and Guidelines

<table>
<thead>
<tr>
<th>Features</th>
<th>Main Layer 3 Interfac e</th>
<th>EFP Interfac e</th>
<th>Trunk EFP Channel</th>
<th>L3 Ethernet Channel</th>
<th>L2 Port Channel</th>
<th>L3 Port Channel Member</th>
<th>L2 Port Channel Member</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>MLPPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>fair-queue</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>priority</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X.7.1</td>
</tr>
<tr>
<td>priority (kbps)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>priority (without queue-limit)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>priority percent</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>queue-limit (bytes)</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X.7.1</td>
</tr>
<tr>
<td>queue-limit (packets)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Ingress Queuing Limitations

The Cisco ASR 903 Series Router does not support queuing on ingress interfaces.

Egress Queuing Limitations

The Cisco ASR 903 Series Router supports tail drop queuing on egress interfaces using the `queue-limit` command. The following limitations apply to egress queuing:

- If you configure a queue size that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.
- Release 3.8 extends the maximum `bytes` value of the `queue-limit number-of-packets [bytes | ms] packets` command. The previous maximum value was 491520 bytes; the new value is 2 MB.
- Release 3.8 enhances the `show policy-map interface` command to display the default queue-limit.
- Release 3.8 introduces support for the `queue-limit percent` command.

Support for Queuing Features on MLPPP Interfaces

Release 3.7(1) introduces support for QoS features on egress MLPPP interfaces. The following queuing features are supported on egress MLPPP interfaces:

- Tail drop queuing using the `queue-limit` command

MLPPP egress queuing is supported only on the 3rd level classes (bottom-most).
Support for Low Latency Queuing on Multiple EFPs


Additional Queuing Limitations

The following additional queuing usage guidelines apply in Release 3.9:

- If you configure a queue size that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.
- The maximum bytes value of the queue-limit number-of-packets [bytes | ms | packets] command is 491520 bytes.
- MLPPP egress queuing is supported only on the 3rd level classes (bottom-most).
- 3-level policies are not supported on MLPPP interfaces.
- CBWFQ is supported on 2nd and 3rd level classes.
- Class-based shaping is supported at all levels.
- Class-based excess bandwidth scheduling is supported on 2nd and 3rd level QoS classes.
- MLPPP egress queuing is supported only on the 3rd level classes (bottom-most).

Congestion Avoidance

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Among the more commonly used congestion avoidance mechanisms is Random Early Detection (RED), which is optimum for high-speed transit networks. Cisco IOS QoS includes an implementation of RED that, when configured, controls when the router drops packets. If you do not configure Weighted Random Early Detection (WRED), the router uses the cruder default packet drop mechanism called tail drop.

Table 13-11 summarizes the QoS congestion avoidance limitations for the Cisco ASR 903 Series Router.

| Table 13-11 Congestion Avoidance QoS Limitations |
### QoS Limitations and Guidelines

#### Features

<table>
<thead>
<tr>
<th>Features</th>
<th>Main Layer 3 Interface</th>
<th>EFP Interface</th>
<th>Trunk EFP</th>
<th>L3 Etherchannel</th>
<th>L2 Port Channel</th>
<th>L3 Port Channel Member</th>
<th>L2 Port Channel Member</th>
<th>OC-3</th>
<th>OC-12</th>
<th>T1/E1</th>
<th>MLPPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Egress</td>
<td>Egress</td>
<td>Egress</td>
<td>Egress</td>
</tr>
<tr>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Egress</td>
<td>Egress</td>
<td>Egress</td>
<td>Egress</td>
</tr>
<tr>
<td>Tail Drop</td>
<td>(default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RED</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>random-detect</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.6</td>
<td>X</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>3.7</td>
</tr>
<tr>
<td>WRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>random-detect</td>
<td>discard-class</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>random-detect</td>
<td>discard-class-based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>random-detect</td>
<td>exponential-weighting-constant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fair-queue</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>precedence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>random-detect</td>
<td>cos-based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>random-detect</td>
<td>dscp-based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco ASR 903 Series Router Chassis Configuration Guide

13-34

OL-25759-03
Configuring Congestion Avoidance

The following sections describe the supported congestion avoidance features on the Cisco ASR 903 Series Router:

- Supported Commands, page 13-35
- Supported Interfaces, page 13-35
- Verifying the Configuration, page 13-37

Supported Commands

The Cisco ASR 903 Series Router supports the following commands for WRED:

- random-detect cos-based—Outer CoS
- random-detect dscp-based—IPv4 DSCP
- random-detect precedence-based—IPv4 Precedence bit

Supported Interfaces

WRED is supported at the PHB level but not on logical or physical interfaces. You can apply WRED policies on the following interface types:

- Main Layer 3 interface
- Port-channel Layer 3 member-links
- Service instances
- Trunk EFPs

Verifying the Configuration

You can use the show policy-map interface command to display the number of WRED drops and tail drops.

For more information about configuring congestion avoidance, see the following documents:
Ingress Congestion Avoidance Limitations

WRED is not supported on ingress interfaces.

Egress Congestion Avoidance Limitations

The following limitations apply when configuring congestion avoidance on the Cisco ASR 903 Series Router:

- WRED is only supported on egress interfaces.
- You must apply WRED within a policy map.
- WRED is not supported in priority queues.
- You can configure a maximum of 2 WRED curves per class.
- You can configure WRED with either the `shape` or the `fair-queue` (CBWFQ) commands.
- The default value for `exponential-weighting-constant` is 9.
- The default value for `mark-probability` is 10.
- You can specify the minimum-threshold and maximum-threshold in terms of bytes or microseconds. Setting threshold values in terms of packets is not supported.

Egress Congestion Avoidance on MLPPP Interfaces

Release 3.7(1) introduces support for the following egress congestion features on MLPPP interfaces:

- RED queuing using the `random-detect` command
- WRED queuing using the `random-detect` command. You can apply WRED to:
  - DSCP
  - Precedence
  - Qos-group
  - Discard-class

MLPPP egress queuing is supported only on the 3rd level classes (bottom-most).

- Class-based Weighted Fair Queuing (CBWFQ) using the `bandwidth` and `bandwidth percent` commands. CBWFQ is supported on 2nd and 3rd level classes.
- Class-based Shaping using the `shape average` and `shape average percent` commands. Class-based shaping is supported at all levels.
- Class-based excess bandwidth scheduling using the `bandwidth remaining percent` and `bandwidth remaining ratio` commands. Class-based excess bandwidth scheduling is supported on 2nd and 3rd level QoS classes.
Additional Congestion Avoidance Limitations

- The following additional congestion avoidance usage guidelines apply in Release 3.9:
- Queuing feature to support WRED in a class such as shape or bandwidth are supported
- You must apply WRED within a policy map.
- WRED is not supported in priority queues.
- You can configure a maximum of 2 WRED curves per class.
- You can configure WRED with either the `shape` or the `fair-queue` (CBWFQ) commands.
- The default value for `exponential-weighting-constant` is 9.
- The default value for `mark-probability` is 10.
- You can specify the minimum-threshold and maximum-threshold in terms of bytes or microseconds. Setting threshold values in terms of packets is not supported.
- Policies using Class-based Weighted Fair Queuing (CBWFQ) and WRED are supported only on individual member links of an etherchannel. Applying a CBWFQ policy directly on an etherchannel interface is not supported.
- WRED is not supported in the class-default class if there are no other user-defined classes in the policy-map.
- Aggregate-WRED is not supported. However, multiple random-detect statements with the same curve are supported in the same class.

Verifying the Configuration

You can use the `show policy-map interface` command to display the number of WRED drops and tail drops.

For more information about configuring congestion avoidance, see the following documents:

Scheduling

This section describes the scheduling limitations and configuration guidelines for the Cisco ASR 903 Series Router.

Ingress Scheduling Limitations

The Cisco ASR 903 Series Router does not support scheduling on ingress interfaces.

Egress Scheduling Limitations

- If you configure a CIR, PIR, or EIR rate that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.
- You can only configure one `priority` value on each parent class applied to a QoS class or logical interface.
- You can only configure priority on one class in a QoS policy.
- You cannot configure `priority` value and a policer in the same class.

The following limitations apply when configuring a 3-level scheduling policy on an egress interface configured as an EFP:

- Only two of the three levels can contain scheduling actions such as `bandwidth`, `shape`, or `priority`.
- One of the levels containing scheduling actions must be the class (bottom) level.

Egress Scheduling on MLPPP Interfaces

Release 3.7(1) introduces support for QoS features on egress MLPPP interfaces including scheduling. The following scheduling features are supported:

- Strict priority using the `priority` command; strict priority is supported on 2nd and 3rd level classes.
- Multi-level priority using the `priority level` command. You can configure two priority levels; the feature is supported on 3rd level classes.

The following limitations apply when configuring a 3-level scheduling policy on an egress interface configured as an EFP:

- Only two of the three levels can contain scheduling actions such as `bandwidth`, `shape`, or `priority`.
- QoS policies using the `priority` command are supported only on individual member links of an etherchannel.
Tracing and Trace Management

This chapter contains the following sections:

- Tracing Overview, page 14-1
- How Tracing Works, page 14-1
- Tracing Levels, page 14-2
- Viewing a Tracing Level, page 14-3
- Setting a Tracing Level, page 14-4
- Viewing the Content of the Trace Buffer, page 14-5

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 Cisco ASR 900 Series Router, which stores tracing files in bootflash:. Trace files are used to store tracing data.

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

- Troubleshooting—If a Cisco ASR 900 Series Router 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 Cisco ASR 900 Series Router. 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 Cisco ASR 900 Series Router. 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” section on page 14-2 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 14-1 shows all of the trace levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

<table>
<thead>
<tr>
<th>Trace Level</th>
<th>Level Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>0</td>
<td>The message is regarding an issue that makes the system unusable.</td>
</tr>
<tr>
<td>Alert</td>
<td>1</td>
<td>The message is regarding an action that must be taken immediately.</td>
</tr>
<tr>
<td>Critical</td>
<td>2</td>
<td>The message is regarding a critical condition. This is the default setting.</td>
</tr>
<tr>
<td>Error</td>
<td>3</td>
<td>The message is regarding a system error.</td>
</tr>
<tr>
<td>Warning</td>
<td>4</td>
<td>The message is regarding a system warning.</td>
</tr>
<tr>
<td>Notice</td>
<td>5</td>
<td>The message is regarding a significant issue, but the router is still working normally.</td>
</tr>
<tr>
<td>Informational</td>
<td>6</td>
<td>The message is useful for informational purposes only.</td>
</tr>
<tr>
<td>Debug</td>
<td>7</td>
<td>The message provides debug-level output.</td>
</tr>
<tr>
<td>Verbose</td>
<td>8</td>
<td>All possible tracing messages are sent.</td>
</tr>
<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 Cisco ASR 900 Series Router 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 Cisco ASR 900 Series Router are set to notice. This setting will be maintained unless changed by a user.

To see the tracing level for any module on the Cisco ASR 900 Series Router, enter the `show platform software trace level` command in privileged EXEC or diagnostic mode.

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

```
Router# show platform software trace level forwarding-manager rp active
Module Name                     Trace Level
-----------------------------------------------
acl                             Notice
binos                           Notice
binos/brand                     Notice
bipc                            Notice
bsignal                         Notice
btrace                          Notice
cce                             Notice
cdllib                          Notice
cef                             Notice
chasfs                          Notice
chasutil                        Notice
erspan                          Notice
ess                             Notice
ether-channel                   Notice
evlib                           Notice
evutil1                          Notice
file_alloc                      Notice
fman_rp                         Notice
fpm                             Notice
fw                              Notice
icmp                            Notice
interfaces                     Notice
iosd                            Notice
ipc                             Notice
ipclog                          Notice
iphc                            Notice
ipsec                           Notice
mgmte-acl                       Notice
```
Setting a Tracing Level

To set a tracing level for any module on the Cisco ASR 900 Series Router, or for all modules within a process on the Cisco ASR 900 Series Router, 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 [uipDr]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipDr]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipDr]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipDr]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipDr]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipDr]: (info): Going to send a status update to the shell manager in slot 0
08/23 11:53:47.417 [uipDr]: (info): Going to send a status update to the shell manager in slot 0
```
Symbols
? command  1-9
<cr>  1-9

Numerics
1-Port Channelized STM-1/OC-3 SPA
    configuring
        SDH mode  10-3

A
administratively down state  7-8
autonegotiation
    configuring  7-6
    disabling on fiber interfaces  7-7
    enabling on fiber interfaces  7-7
auxiliary port, using  1-7

B
Bidirectional Forwarding Detection (BFD)  4-3

C
carriage return (<cr>)  1-9
CEF  12-1
CEF for PFC2
    See CEF
circuit emulation service over packet-switched network  12-3
Cisco IOS configuration changes, saving  1-12
command-line interface, getting help  1-8
command line processing  1-8
command modes, understanding  1-1 to 1-2
    commands
        context-sensitive help for abbreviating  1-9
        default form, using  1-12
        no form, using  1-12
    command syntax
        displaying (example)  1-9
configuration files, backing up to bootflash  1-12
configuration files, backing up to TFTP  1-13
configuration files, backing up to USB Flash Disk  1-13
configuration files, managing  1-12
configurations, saving  1-12
configure terminal command  7-2
crashinfo files, overview  5-5
CRC size, configuring  10-17
configuring
        SDH mode  10-3
core, accessing  1-4
console, accessing using a direct connection  1-4
core, accessing using telnet  1-6
core, configuring a transport map  2-3
core, connecting  1-4
core, traffic handling  2-2
core, using  1-5
core, viewing handling configuration  2-11
copy command  7-7

D
diagnostic configuration mode, summary of  1-3
diagnostic mode, overview  1-3
dot1q encapsulation  7-6
configuration (example) 7-15

e1 bert pattern command 8-12
encapsulation
    configuring 10-16
    dot1q 7-6
    configuration (example) 7-15
    SNAP 7-5

file systems, overview 5-2
filtering output, show and more commands 1-14
for 7-10
framing, configuring 8-5

Gigabit Ethernet Interface Modules
    configuring 7-1
    modifying MTU 7-5
global configuration mode, summary of 1-2

hardware platforms
    See platforms, supported
help command 1-9
history buffer, using 1-8
Hot Standby Router Protocol. See HSRP.
HSRP, verifying configuration 7-4

IEEE 802.1Q encapsulation 7-6
    configuration (example) 7-15

interface
    basic configuration (example) 7-14
    enabling 7-3
    restarting 7-8
    shutting down 7-8
    verifying configuration 7-9 to ??
interface address, specifying 7-3
interface configuration mode, summary of 1-2
interface gigabitethernet command 7-2
interface tengigabitethernet command 7-2
ip address command 7-2

keyboard shortcuts 1-8

lost+found directory, overview 5-5

Management Ethernet Interface, common tasks 3-3
Management Ethernet interface, interface numbering 3-1
Management Ethernet interface, IP Address Handling 3-2
Management Ethernet interface, overview 3-1
Management Ethernet Interface, VRF 3-2
modem, accessing 1-7
modes
    See command modes
mpls mtu command 7-5
MTU (maximum transmission unit)
    configuration (example) 7-14
    default size 7-5
interface MTU
    additional overhead 7-5
    configuration guidelines 7-5
    configuring 7-5
IP MTU, description 7-5
maximum size 7-5
MPLS MTU, description 7-5
tag MTU, description 7-5
types 7-5
mtu command 7-2, 7-3, 7-6

N
negotiation auto command 7-7
no negotiation auto command 7-7
no shut command 7-3
NVRAM 7-7

O
OIR (online insertion and removal)
and shutting down or restarting interfaces 7-8
online insertion and removal. See OIR.

P
platforms, supported
release notes, identify using 1-15
privileged EXEC mode, summary of 1-2
prompts, system 1-2
provisioning files, overview 5-2

Q
question mark (?) command 1-9

R
release notes
See platforms, supported
ROM monitor mode, summary of 1-3
RPAccess, Overview 5-2
RPBase, Overview 5-2
RPControl, Overview 5-2
RPIOs, Overview 5-2
RP Memory Recommendations 5-3
running configuration, saving to NVRAM 7-7

S
SDH mode, configuring 10-3
Secure Shell (SSH), configuring persistent SSH 2-8
Secure Shell (SSH), persistent 2-2
Secure Shell (SSH), persistent SSH restrictions 2-16
Secure Shell (SSH), viewing handling configuration 2-11
show history command 1-8
show hw-module subslot transceiver idprom command 7-10
show interface serial command 8-14
show interfaces gigabitethernet command 7-6
show standby command 7-4
shutdown command 7-8
SNAP (Subnetwork Access Protocol) encapsulation 7-5
Stateful Switchover, Supported Protocols and Applications 4-2
Stateful Switchover (SSO), overview 4-2
Step1 12-11
Step4 12-12
Structure-agnostic TDM over Packet 12-2
Structure-agnostic TDM over Packet (SaToP) 12-2

T
T1/E1 Interface Module 8-1
configuring 8-2
framing 8-5
verifying the configuration 8-14
Tab key, command completion 1-9
telnet, configuring persistent telnet 2-5
Index

telnet, persistent  2-2
telnet, persistent telnet restrictions  2-16
telnet, using  1-6
telnet, using to access console  1-6
telnet, viewing handling configuration  2-11
Tracing, how tracing works  14-1
Tracing, overview  14-1
Tracing, setting a tracing level  14-4
Tracing, tracing levels  14-2
Tracing, viewing a tracing level  14-3
Tracing, viewing trace logs  14-5

U

user EXEC mode, summary of  1-2

V

VLANs (virtual LANs)
configuration (example)  7-15