



# 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 i](#)
- [Document Revision History, page i](#)
- [Organization, page ii](#)
- [Related Documentation, page ii](#)
- [Document Conventions, page iii](#)
- [Obtaining Documentation and Submitting a Service Request, page iv](#)

## Objectives

This document provides an overview of software functionality that is specific to the Cisco ASR 903 Series Router. It is not intended as a comprehensive guide to all of the software features that can be run using the Cisco ASR 903 Series Router, but only the software aspects that are specific to this platform.

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

## Document Revision History

The Document Revision History records technical changes to this document. The table shows the Cisco IOS XE software release number and document revision number for the change, the date of the change, and a brief summary of the change.

Release No.	Date	Change Summary
IOS XE 3.5s	November 2011	First release.
IOS XE 3.5s	February 2012	Added Installing and Upgrading Software chapter.
IOS XE 3.5.1s	February 2012	Added information about QoS ACL feature.
IOS XE 3.5.2	April 2012	Added information about egress QoS marking feature.

# Organization

This document contains the following chapters:

Chapter	Title	Description
1	<a href="#">Using Cisco IOS XE Software</a>	Provides an introduction to accessing the command-line interface (CLI) and using the Cisco software and related tools.
2	<a href="#">Console Port, Telnet, and SSH Handling</a>	Provides an overview and configuration options for the handling of incoming console port, telnet, and SSH traffic.
3	<a href="#">Using the Management Ethernet Interface</a>	Provides an overview and configuration options for the Management Ethernet interface.
4	<a href="#">High Availability Overview</a>	Provides an overview of the High Availability architecture, behavior, and features.
5	<a href="#">Installing and Upgrading Software</a>	Provides instructions on how to install and upgrade software and firmware on the router.
6	<a href="#">Configuring the Route Switch Processor</a>	Provides information on configuring the Route Switch Processor (RSP).
7	<a href="#">Configuring Ethernet Interfaces</a>	Provides information on configuring the Ethernet Interface Module.
8	<a href="#">Configuring T1/E1 Interfaces</a>	Provides information on configuring the T1/E1 Interface Module.
9	<a href="#">Configuring Clocking and Timing</a>	Provides information on configuring clocking and timing features.
10	<a href="#">Configuring Synchronous Ethernet ESMC and SSM</a>	Provides information on configuring Synchronous Ethernet clock synchronization features.
11	<a href="#">Configuring Pseudowire</a>	Provides information on configuring MPLS pseudowire features.
12	<a href="#">Configuring Quality of Service</a>	Provides information on configuring QoS features.
13	<a href="#">Tracing and Trace Management</a>	Provides an overview of tracing on the Cisco and how to manage the tracing process and files.

*The following table is conditioned for the Catalyst 6500 Series Switch for SX release.*

## Related Documentation

This section refers you to other documentation that also might be useful as you configure your Cisco ASR 903 Series Router. The documentation listed below is available online.

## Cisco ASR 903 Series Router Documentation

The documentation homepage for the Cisco ASR 903 Series Router is:

[http://www.cisco.com/en/US/products/ps11610/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11610/tsd_products_support_series_home.html)

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

[http://cisco.com/en/US/products/ps9587/tsd\\_products\\_support\\_series\\_home.html](http://cisco.com/en/US/products/ps9587/tsd_products_support_series_home.html)

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:

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

Command syntax descriptions use the following conventions:

Convention	Description
<b>bold</b>	Bold text indicates commands and keywords that you enter exactly as shown.
<i>italics</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x   y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

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

Convention	Description
[x {y   z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
screen	Examples of information displayed on the screen are set in Courier font.
<b>bold screen</b>	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	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.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:



**Caution**

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



**Note**

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:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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 903 Series Router:

- [Understanding Command Modes, page 1-2](#)
- [Understanding Diagnostic Mode, page 1-3](#)
- [Accessing the CLI Using a Router Console, page 1-4](#)
- [Using the Auxiliary Port, page 1-7](#)
- [Using Keyboard Shortcuts, page 1-7](#)
- [Using the History Buffer to Recall Commands, page 1-8](#)
- [Getting Help, page 1-9](#)
- [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 1-1** Accessing and Exiting Command Modes

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

Table 1-1 Accessing and Exiting Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
Diagnostic	<p>The router boots up or accesses diagnostic mode in the following scenarios:</p> <ul style="list-style-type: none"> <li>In some cases, diagnostic mode will be reached when the IOS process or processes fail. In most scenarios, however, the router will reload.</li> <li>A user-configured access policy was configured using the <b>transport-map</b> command that directed the user into diagnostic mode. See the “<a href="#">Console Port, Telnet, and SSH Handling</a>” chapter of this book for information on configuring access policies.</li> <li>The router was accessed using a Route Switch Processor auxiliary port.</li> <li>A break signal (<b>Ctrl-C</b>, <b>Ctrl-Shift-6</b>, or the <b>send break</b> command) was entered and the router was configured to go into diagnostic mode when the break signal was received.</li> </ul>	Router (diag) #	<p>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.</p> <p>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.</p> <p>If the router is accessed through the Route Switch Processor auxiliary port, access the router through another port. Accessing the router through the auxiliary port is not useful for customer purposes anyway.</p>
ROM monitor	From privileged EXEC mode, use the <b>reload EXEC</b> command. Press the <b>Break</b> key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the <b>continue</b> command.

## Understanding Diagnostic Mode

Diagnostic mode is supported on the Cisco ASR 903 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.

- 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 903 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 Router 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 1-5](#)
- [Accessing the CLI from a Remote Console Using a Modem, page 1-7](#)



**Note**

For more information about connecting cables to the router, see the [Cisco ASR 903 Hardware Installation Guide](#).



**Note**

For information about installing USB devices drivers in order to use the USB console port, see the [Cisco ASR 903 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 903 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 (vty) using the **line vty** global configuration command. You also should configure the vty 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”:

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



### Note

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

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

```
Router> enable
```

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

```
Password: enablepass
```

**Step 5** When the 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 Telnet session, use the **exit** or **logout** command as shown in the following example:

```
Router# logout
```

---

## Accessing the CLI from a Remote Console Using a Modem

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

The console port on a Cisco ASR 903 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 [Cisco ASR 903 Hardware Installation Guide](#).

## 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 1-2 Keyboard Shortcuts**

Keystrokes	Purpose
<b>Ctrl-B</b> or the <b>Left Arrow</b> key <sup>1</sup>	Move the cursor back one character
<b>Ctrl-F</b> or the <b>Right Arrow</b> key <sup>1</sup>	Move the cursor forward one character
<b>Ctrl-A</b>	Move the cursor to the beginning of the command line
<b>Ctrl-E</b>	Move the cursor to the end of the command line
<b>Esc B</b>	Move the cursor back one word
<b>Esc F</b>	Move the cursor forward one word

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

## Using the History Buffer to Recall Commands

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

Table 1-3 lists the history substitution commands.

**Table 1-3 History Substitution Commands**

Command	Purpose
<b>Ctrl-P</b> or the <b>Up Arrow</b> key <sup>1</sup>	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
<b>Ctrl-N</b> or the <b>Down Arrow</b> key <sup>1</sup>	Return to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the <b>Up Arrow</b> key.
Router# <b>show history</b>	While in EXEC mode, list the last several commands you have just entered.

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

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

## Finding Command Options Example

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

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 shows examples of how you can use the question mark (?) to assist you in entering commands.

**Table 1-5** Finding Command Options

Command	Comment
Router> <b>enable</b> Password: <password> Router#	Enter the <b>enable</b> command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a “#” from the “>”; for example, Router> to Router#.
Router# <b>configure terminal</b> Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter the <b>configure terminal</b> privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.

Table 1-5 Finding Command Options (continued)

Command	Comment
<pre>Router(config)# <b>interface serial</b> ? &lt;0-6&gt;      Serial interface number Router(config)# <b>interface serial 4</b> ? / Router(config)# <b>interface serial 4/</b> ? &lt;0-3&gt;      Serial interface number Router(config)# <b>interface serial 4/0</b> ? &lt;cr&gt; Router(config)# <b>interface serial 4/0</b> Router(config-if)#</pre>	<p>Enter interface configuration mode by specifying the serial interface that you want to configure using the <b>interface serial</b> global configuration command.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.</p> <p>When the &lt;cr&gt; symbol is displayed, you can press <b>Enter</b> to complete the command.</p> <p>You are in interface configuration mode when the prompt changes to Router(config-if)#.</p>
<pre>Router(config-if)# ? Interface configuration commands: . . . ip                Interface Internet Protocol config com- mands keepalive         Enable keepalive lan-name          LAN Name command llc2              LLC2 Interface Subcommands load-interval    Specify interval for load calculation for an interface locaddr-priority Assign a priority group logging          Configure logging for interface loopback         Configure internal loopback on an in- terface mac-address       Manually set interface MAC address mls              mls router sub/interface commands mpoa             MPOA interface configuration commands mtu              Set the interface Maximum Transmission Unit (MTU) netbios          Use a defined NETBIOS access list or enable name-caching no               Negate a command or set its defaults nrzi-encoding    Enable use of NRZI encoding ntp              Configure NTP . . . Router(config-if)#</pre>	<p>Enter ? to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.</p>

Table 1-5 Finding Command Options (continued)

Command	Comment
<pre>Router(config-if)# ip ? Interface IP configuration subcommands:   access-group      Specify access control for packets   accounting         Enable IP accounting on this interface   address           Set the IP address of an interface   authentication    authentication subcommands   bandwidth-percent Set EIGRP bandwidth limit   broadcast-address Set the broadcast address of an inter-   face   cgmp              Enable/disable CGMP   directed-broadcast Enable forwarding of directed broad-   casts   dvmrp            DVMRP interface commands   hello-interval   Configures IP-EIGRP hello interval   helper-address   Specify a destination address for UDP   broadcasts   hold-time        Configures IP-EIGRP hold time   .   .   . Router(config-if)# ip</pre>	<p>Enter the command that you want to configure for the interface. This example uses the <b>ip</b> command.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p>
<pre>Router(config-if)# ip address ?   A.B.C.D          IP address   negotiated       IP Address negotiated over PPP Router(config-if)# ip address</pre>	<p>Enter the command that you want to configure for the interface. This example uses the <b>ip address</b> command.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you must enter an IP address or the <b>negotiated</b> keyword.</p> <p>A carriage return (&lt;cr&gt;) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 ?   A.B.C.D          IP subnet mask Router(config-if)# ip address 172.16.0.1</pre>	<p>Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.</p> <p>A &lt;cr&gt; is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?   secondary       Make this IP address a secondary ad-   dress   &lt;cr&gt; Router(config-if)# ip address 172.16.0.1 255.255.255.0</pre>	<p>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you can enter the <b>secondary</b> keyword, or you can press <b>Enter</b>.</p> <p>A &lt;cr&gt; is displayed; you can press <b>Enter</b> to complete the command, or you can enter another keyword.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	<p>In this example, <b>Enter</b> is pressed to complete the command.</p>

## 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 903 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 903 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
```



```

45313 drwx      4096 Nov 17 2011 17:36:12 +05:30 core
75521 drwx      4096 Feb 2 2000 13:35:11 +05:30 .prst_sync
90625 drwx      4096 Feb 2 2000 13:35:22 +05:30 .rollback_timer
105729 drwx      8192 Nov 21 2011 22:57:55 +05:30 tracelogs
30209 drwx      4096 Feb 2 2000 13:36:17 +05:30 .installer

```

1339412480 bytes total (1199448064 bytes free)

```

Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?

```

3517 bytes copied in 0.647 secs (5436 bytes/sec)

```

Router# dir bootflash:
Directory of bootflash:/

```

```

   11 drwx      16384 Feb 2 2000 13:33:40 +05:30 lost+found
15105 drwx      4096 Feb 2 2000 13:35:07 +05:30 .ssh
45313 drwx      4096 Nov 17 2011 17:36:12 +05:30 core
75521 drwx      4096 Feb 2 2000 13:35:11 +05:30 .prst_sync
90625 drwx      4096 Feb 2 2000 13:35:22 +05:30 .rollback_timer
   12 -rw-         0 Feb 2 2000 13:36:03 +05:30 tracelogs.878
105729 drwx      8192 Nov 21 2011 23:02:13 +05:30 tracelogs
30209 drwx      4096 Feb 2 2000 13:36:17 +05:30 .installer
   13 -rw-      1888 Nov 21 2011 23:03:17 +05:30 startup-config

```

1339412480 bytes total (1199439872 bytes free)

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

```

Router# dir usb0:
Directory of usb0:/

```

```

43261 -rwx    208904396 May 27 2008 14:10:20 -07:00
asr903rsp1-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
asr903rsp1-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-config]? /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

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

## Powering Off the Router

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

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

The following screenshot shows an example of this process:

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

*Jun 18 19:38:21.870: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
command.
```

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

## Finding Support Information for Platforms and Cisco Software Images

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

## Using Cisco Feature Navigator

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

## Using Software Advisor

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

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

## Using Software Release Notes

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

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

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





## Console Port, Telnet, and SSH Handling

---

This chapter covers the following topics:

- [Console Port Overview for the Cisco ASR 903 Series Router, page 2-1](#)
- [Console Port Handling Overview, page 2-2](#)
- [Telnet and SSH Overview for the Cisco ASR 903 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 2-9](#)
- [Viewing Console Port, SSH, and Telnet Handling Configurations, page 2-12](#)
- [Important Notes and Restrictions, page 2-17](#)

### Console Port Overview for the Cisco ASR 903 Series Router

The console port on the Cisco ASR 903 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 Directly-Connected Console” section on page 1-4](#).

### Connecting Console Cables

For information about connecting console cables to the Cisco ASR 903 Series Router, see the [Cisco ASR 903 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](#).

## 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 903 Series Router

Telnet and Secure Shell (SSH) on the Cisco ASR 903 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](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 903 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 903 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](#).

See the [“Configuring Persistent Telnet” section on page 2-5](#) and the [“Configuring Persistent SSH” section on page 2-9](#) for information on the various other options that are configurable using persistent Telnet or persistent SSH transport maps.


# Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the Cisco ASR 903 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*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>transport-map type console transport-map-name</b></p> <p><b>Example:</b> Router(config)# transport-map type console consolehandler</p>	<p>Creates and names a transport map for handling console connections, and enter transport map configuration mode.</p>
Step 4	<p><b>connection wait [allow interruptible   none]</b></p> <p><b>Example:</b> Router(config-tmap)# connection wait none</p>	<p>Specifies how a console connection will be handled using this transport map:</p> <ul style="list-style-type: none"> <li><b>allow interruptible</b>—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.</li> </ul> <p> <b>Note</b> Users can interrupt a waiting connection by entering <b>Ctrl-C</b> or <b>Ctrl-Shift-6</b>.</p> <ul style="list-style-type: none"> <li><b>none</b>—The console connection immediately enters diagnostic mode.</li> </ul>
Step 5	<p><b>banner [diagnostic   wait] banner-message</b></p> <p><b>Example:</b> Router(config-tmap)# banner diagnostic X Enter TEXT message. End with the character 'X'. --Welcome to Diagnostic Mode-- X Router(config-tmap)#</p>	<p>(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.</p> <ul style="list-style-type: none"> <li><b>diagnostic</b>—Creates a banner message seen by users directed into diagnostic mode as a result of the console transport map configuration.</li> <li><b>wait</b>—Creates a banner message seen by users waiting for the IOS vty to become available.</li> <li><i>banner-message</i>—The banner message, which begins and ends with the same delimiting character.</li> </ul>



	Command or Action	Purpose
Step 6	<b>exit</b>  <b>Example:</b> Router(config-tmap)# exit	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	<b>transport type console</b> <i>console-line-number</i> <b>input</b> <i>transport-map-name</i>  <b>Example:</b> Router(config)# transport type console 0 input consolehandler	Applies the settings defined in the transport map to the console interface.  The <i>transport-map-name</i> for this command must match the <i>transport-map-name</i> defined in the <b>transport-map type console</b> command.

## Examples

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

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

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

## Configuring Persistent Telnet

This task describes how to configure persistent Telnet on the Cisco ASR 903 Series Router.

### Prerequisites


For a persistent Telnet connection to access an IOS vty line on the Cisco ASR 903 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*

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

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>transport-map type persistent telnet</b> <i>transport-map-name</i>  <b>Example:</b> Router(config)# transport-map type persistent telnet telnethandler	Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.
Step 4	<b>connection wait [allow {interruptible}   none {disconnect}]</b>  <b>Example:</b> Router(config-tmap)# connection wait none	Specifies how a persistent Telnet connection will be handled using this transport map: <ul style="list-style-type: none"> <li><b>allow</b>—The Telnet connection waits for an IOS vty line to become available, and exits the router if interrupted.</li> <li><b>allow interruptible</b>—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.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p><b>Note</b> Users can interrupt a waiting connection by entering <b>Ctrl-C</b> or <b>Ctrl-Shift-6</b>.</p> </div> <ul style="list-style-type: none"> <li><b>none</b>—The Telnet connection immediately enters diagnostic mode.</li> <li><b>none disconnect</b>—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.</li> </ul>
Step 5	<b>banner [diagnostic   wait] banner-message</b>  <b>Example:</b> Router(config-tmap)# banner diagnostic X Enter TEXT message. End with the character 'X'. --Welcome to Diagnostic Mode-- X Router(config-tmap)#	(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS vty line as a result of the persistent Telnet configuration. <ul style="list-style-type: none"> <li><b>diagnostic</b>—creates a banner message seen by users directed into diagnostic mode as a result of the persistent Telnet configuration.</li> <li><b>wait</b>—creates a banner message seen by users waiting for the vty line to become available.</li> <li><i>banner-message</i>—the banner message, which begins and ends with the same delimiting character.</li> </ul>

	Command or Action	Purpose
Step 6	<pre>transport interface gigabitethernet 0</pre> <p><b>Example:</b> Router(config-tmap)# transport interface gigabitethernet 0</p>	<p>Applies the transport map settings to the Management Ethernet interface (interface gigabitethernet 0).</p> <p>Persistent Telnet can only be applied to the Management Ethernet interface on the Cisco ASR 903 Series Router. This step must be taken before applying the transport map to the Management Ethernet interface.</p>
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(config-tmap)# exit</p>	<p>Exits transport map configuration mode to re-enter global configuration mode.</p>
Step 8	<pre>transport type persistent telnet input transport-map-name</pre> <p><b>Example:</b> Router(config)# transport type persistent telnet input telnethandler</p>	<p>Applies the settings defined in the transport map to the Management Ethernet interface.</p> <p>The <i>transport-map-name</i> for this command must match the <i>transport-map-name</i> defined in the <b>transport-map type persistent telnet</b> command.</p>

## Examples

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

A diagnostic and a wait banner are also configured.

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

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

Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```


# Configuring Persistent SSH

This task describes how to configure persistent SSH on the Cisco ASR 903 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

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>transport-map type persistent ssh</b> <i>transport-map-name</i></p> <p><b>Example:</b> Router(config)# transport-map type persistent ssh sshhandler</p>	<p>Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode.</p>
Step 4	<p><b>connection wait</b> [<b>allow</b> {<b>interruptible</b>}   <b>none</b> {<b>disconnect</b>}]</p> <p><b>Example:</b> Router(config-tmap)# connection wait allow interruptible</p>	<p>Specifies how a persistent SSH connection will be handled using this transport map:</p> <ul style="list-style-type: none"> <li><b>allow</b>—The SSH connection waits for the vty line to become available, and exits the router if interrupted.</li> <li><b>allow interruptible</b>—The SSH connection waits for the vty line to become available, and also allows users to enter diagnostic mode by interrupting a SSH connection waiting for the vty line to become available. This is the default setting.</li> </ul> <p> <b>Note</b> Users can interrupt a waiting connection by entering <b>Ctrl-C</b> or <b>Ctrl-Shift-6</b>.</p> <ul style="list-style-type: none"> <li><b>none</b>—The SSH connection immediately enters diagnostic mode.</li> <li><b>none disconnect</b>—The SSH connection does not wait for the vty line from IOS and does not enter diagnostic mode, so all SSH connections are rejected if no vty line is immediately available.</li> </ul>
Step 5	<p><b>rsa keypair-name</b> <i>rsa-keypair-name</i></p> <p><b>Example:</b> Router(config-tmap)# rsa keypair-name sshkeys</p>	<p>Names the RSA keypair to be used for persistent SSH connections.</p> <p>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 <b>ip ssh rsa keypair-name</b> command, do not apply to persistent SSH connections.</p> <p>No <i>rsa-keypair-name</i> is defined by default.</p>

	Command or Action	Purpose
Step 6	<p><b>authentication-retries</b> <i>number-of-retries</i></p> <p><b>Example:</b> Router(config-tmap)# authentication-retries 4</p>	<p>(Optional) Specifies the number of authentication retries before dropping the connection.</p> <p>The default <i>number-of-retries</i> is 3.</p>
Step 7	<p><b>banner</b> [<b>diagnostic</b>   <b>wait</b>] <i>banner-message</i></p> <p><b>Example:</b> Router(config-tmap)# banner diagnostic X Enter TEXT message. End with the character 'X'. --Welcome to Diagnostic Mode-- X Router(config-tmap)#</p>	<p>(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.</p> <ul style="list-style-type: none"> <li>• <b>diagnostic</b>—Creates a banner message seen by users directed into diagnostic mode as a result of the persistent SSH configuration.</li> <li>• <b>wait</b>—Creates a banner message seen by users waiting for the vty line to become active.</li> <li>• <i>banner-message</i>—The banner message, which begins and ends with the same delimiting character.</li> </ul>
Step 8	<p><b>time-out</b> <i>timeout-interval</i></p> <p><b>Example:</b> Router(config-tmap)# time-out 30</p>	<p>(Optional) Specifies the SSH time-out interval in seconds.</p> <p>The default <i>timeout-interval</i> is 120 seconds.</p>
Step 9	<p><b>transport interface gigabitethernet 0</b></p> <p><b>Example:</b> Router(config-tmap)# transport interface gigabitethernet 0</p>	<p>Applies the transport map settings to the Management Ethernet interface (interface gigabitethernet 0).</p> <p>Persistent SSH can only be applied to the Management Ethernet interface on the Cisco ASR 903 Series Router.</p>
Step 10	<p><b>exit</b></p> <p><b>Example:</b> Router(config-tmap)# exit</p>	<p>Exits transport map configuration mode to re-enter global configuration mode.</p>
Step 11	<p><b>transport type persistent ssh input</b> <i>transport-map-name</i></p> <p><b>Example:</b> Router(config)# transport type persistent ssh input sshhandler</p>	<p>Applies the settings defined in the transport map to the Management Ethernet interface.</p> <p>The <i>transport-map-name</i> for this command must match the <i>transport-map-name</i> defined in the <b>transport-map type persistent ssh</b> command.</p>

## Examples

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

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

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

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

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

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

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)#banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for vty line--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

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

## Viewing Console Port, SSH, and Telnet Handling Configurations

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

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

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

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for the IOS CLI

  bshell banner:

Welcome to Diagnostic Mode
```



```
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS prompt

  Bshell banner:

Welcome to Diagnostic Mode

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

Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS process

  Bshell banner:

Welcome to Diagnostic Mode

Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport

Connection:
  Wait option: Wait Allow

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

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for the IOS CLI

  Bshell banner:

Welcome to Diagnostic Mode
```

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

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS prompt

  Bshell banner:

Welcome to Diagnostic Mode

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

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

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS process

  Bshell banner:

Welcome to Diagnostic Mode

Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport

Connection:
  Wait option: Wait Allow

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

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
```

```
Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode

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

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode

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

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode

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

Router#
```

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

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

Method      : telnet
Rule        : wait
Shell banner:
```

```

Wait banner :

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

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

```

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

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

```

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

Method      : telnet
Rule        : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process

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

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

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

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

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

```

```
Method      : telnet
Rule        : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode
```

```
Wait banner :
Waiting for IOS process
```

```
Method      : ssh
Rule        : wait with interrupt
Shell banner:
Welcome to Diag Mode
```

```
Wait banner :
Waiting for IOS
```

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

## 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 3-2](#)
- [Gigabit Ethernet Port Numbering, page 3-2](#)
- [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 903 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. This is discussed in more detail in the [“Gigabit Ethernet Management Interface VRF”](#) section on page 3-2.

## 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 903 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 903 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 903 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 903 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 903 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 3-5](#)
- [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 3-6](#)
- [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 3-7](#)

## Viewing the VRF Configuration

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

This example shows the default VRF configuration:

```
Router# show running-config vrf
Building configuration...

Current configuration : 351 bytes
vrf definition Mgmt-intf
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
```

```

exit-address-family
!
(some output removed for brevity)

```

## Viewing Detailed VRF Information for the Management Ethernet VRF

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

```

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

```

## Setting a Default Route in the Management Ethernet Interface VRF

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

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

## Setting the Management Ethernet IP Address

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

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

### IPv4 Example

```

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

```

### IPv6 Example

```

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

```

## Telnetting over the Management Ethernet Interface

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

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

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

## Pinging over the Management Ethernet Interface

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

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

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

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

## Copy Using TFTP or FTP

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

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

### TFTP Example

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

### FTP Example

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

## NTP Server

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

The following CLI provides an example of this procedure.

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

## SYSLOG Server

To specify the Management Ethernet interface as the source 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.

- 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 4-1 Hardware Redundancy Overview**

Hardware	Support for Dual Hardware Configuration	Failover Behavior
Route Switch Processor	Yes	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.
Interface module	No	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.

## 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 5-6](#)
- [Understanding In-Service Software Upgrades, page 5-6](#)
- [Downloading an Image, page 5-7](#)
- [Setting the Router to Boot in Sub-Package Mode, page 5-7](#)
- [Completing a Single Command Software Upgrade, page 5-9](#)
- [Software Upgrade Examples, page 5-10](#)

### Software Packaging on the Cisco ASR 903 Series Router

This section covers the following topics:

- [Cisco ASR 903 Series Router Software Overview, page 5-1](#)
- [Provisioning Files, page 5-2](#)
- [Upgrading Field Programmable Hardware Devices, page 5-2](#)

### Cisco ASR 903 Series Router Software Overview

The Cisco IOS XE software supports two software installation types:

- **Consolidated image**—A single software image containing a full collection of software packages. Consolidated mode provides a simplified installation and can be stored in bootflash, a TFTP server, or a network server. Consolidated mode is not supported on the Cisco ASR 903 Series Router.
- **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 Cisco ASR 903 Series Router supports sub-package mode.

**Caution**

The Cisco ASR 903 Series Router supports sub-package mode; consolidated mode is not supported.

## Understanding Cisco ASR 903 Series Router Software Packages

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

**Table 5-1 Individual Sub-Packages**

Sub-Package	Purpose
RPBase	Route Switch Processor (RSP) operating system
RPControl	Control plane processes between IOS process and the rest of the platform.
RPAccess	Handles security features including Secure Socket Layer (SSL) and Secure Shell (SSH)
RPIOS	Cisco IOS kernel, which is where IOS features are stored and run. <b>Note</b> Each consolidated image has a unique RPIOS package.
FP Pkg	Controls FP daemons.
IO Pkg	Controls input/output driver daemons.
LC Base	Controls basic kernel functions including runtime, initialization scripts, and chassis control daemons.

## Provisioning Files

Provisioning files manage the boot process when the Cisco ASR 903 Series Router is configured to run using individual 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.

## Upgrading Field Programmable Hardware Devices

Cisco IOS XE supports upgradeable firmware for field programmable hardware devices such as interface modules (IMs). Generally an upgrade is only necessary in cases where a system message indicates that an upgrade is required or a Cisco technical support representative suggests an upgrade.

The procedures in this chapter describe how to upgrade the firmware on Cisco ASR 903 Series Router.

## File Systems on the Cisco ASR 903 Series Router

Table 5-2 provides a list of file systems that can be seen on the Cisco ASR 903 Series Router.

**Table 5-2 File Systems**

File System	Description
bootflash:	The boot flash memory file system on the active RSP.
cns:	The Cisco Networking Services file directory.

**Table 5-2** *File Systems (continued)*

<b>File System</b>	<b>Description</b>
nvrn:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
stby-bootflash:	The boot flash memory file system on the standby RSP.
stby-harddisk:	The hard disk file system on the standby RSP.
stby-usb[0-1]:	The Universal Serial Bus (USB) flash drive file systems on the standby RSP.
system:	The system memory file system, which includes the running configuration.
tar:	The archive file system.
tmpsys:	The temporary system files file system.
usb[0-1]:	The Universal Serial Bus (USB) flash drive file systems on the active RSP.

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.

## Bootflash Space Requirements

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

## System Requirements

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

- [RP Memory Recommendations, page 5-4](#)
- [ROMmon Version Requirements, page 5-5](#)
- [Determining the Software Version, page 5-5](#)
- [Cisco IOS XE 3S to Cisco IOS Version Number Mapping, page 5-5](#)

## RP Memory Recommendations

The Cisco IOS XE 3S images and packages available vary based on the route processor installed in the system.

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

**Table 3** Memory Recommendations for the Cisco ASR 903 Series Router Consolidated Package Image

Platform	Image Name	Software Image	Individual Subpackage Contents	DRAM Memory
Cisco ASR 903 Router	Cisco ASR 903 Series RSP1 UNIVERSAL W/O CRYPTO	asr903rsp1-universal. <i>version</i> .bin	asr903rsp1-rpbase. <i>version</i> .pkg	2 GB (RSP1)
			asr903rsp1-rpcontrol. <i>version</i> .pkg	4 GB (RSP1+)
			asr903rsp1-rpaccess. <i>version</i> .pkg	
			asr903rsp1-rpios-universal. <i>version</i> .pkg	
			asr903rsp1-espbase. <i>version</i> .pkg	
			asr903rsp1-sipbase. <i>version</i> .pkg	
			asr903rsp1-sipspa. <i>version</i> .pkg	
			asr903rsp1-packages-universal. <i>version</i> .conf	
			packages.conf	
Cisco ASR 903 Router	Cisco ASR 903 Series RSP1 UNIVERSAL	asr903rsp1-universalk9. <i>version</i> .bin	asr903-hw-programmables. <i>version</i> .pkg	2 GB (RSP1)
			asr903rsp1-espbase. <i>version</i> .pkg	4 GB (RSP1+)
			asr903rsp1-packages-universalk9. <i>version</i> .conf	
			asr903rsp1-rpaccess. <i>version</i> .pkg	
			asr903rsp1-rpbase. <i>version</i> .pkg	
			asr903rsp1-rpcontrol. <i>version</i> .pkg	
			asr903rsp1-rpios-universalk9. <i>version</i> .pkg	
			asr903rsp1-sipbase. <i>version</i> .pkg	
			asr903rsp1-sipspa. <i>version</i> .pkg	
packages.conf				

**Table 3** Memory Recommendations for the Cisco ASR 903 Series Router Consolidated Package Image

Platform	Image Name	Software Image	Individual Subpackage Contents	DRAM Memory
Cisco ASR 903 Router	Cisco ASR 903 Series RSP1 UNIVERSAL NPE	asr903rsp1-universalk9_npe. version.bin	asr903-hw-programmables.version.pkg	2 GB (RSP1) 4 GB (RSP1+)
			asr903rsp1-espbase.version.pkg	
			asr903rsp1-packages-universalk9.version.conf	
			asr903rsp1-rpaccess.version.pkg	
			asr903rsp1-rpbase.version.pkg	
			asr903rsp1-rpcontrol.version.pkg	
			asr903rsp1-rpios-universalk9_npe.version.pkg	
			asr903rsp1-sipbase.version.pkg	
			asr903rsp1-sipspa.version.pkg	
			packages.conf	

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

Cisco IOS XE 3S Version	Cisco IOS Version
3.5.0S	15.2(1)S
3.5.1S	15.2(1)S1
3.6.0S	15.2(2)S
3.6.1S	15.2(2)S1
3.7.0S	15.2(4)S

The Cisco ASR 903 Series Router does not support IOS XE versions prior to 3.50S.

# 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*

File or Directory	Description
crashinfo files	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.
core files	The bootflash/core directory is the storage area for .core files.   <b>Caution</b> Do not erase or move the core directory.
lost+found directory	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.
tracelogs files	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.   <b>Caution</b> Do not erase or move the tracelog directory.

## Understanding In-Service Software Upgrades

The in-service software upgrade (ISSU) process allows you to update the router software with minimal service interruption. The following sections describe the ISSU process on the Cisco ASR 903 Series Router:

- [Restrictions for an ISSU Upgrade, page 5-6](#)
- [Single-Command Upgrade Overview, page 5-7](#)

## Restrictions for an ISSU Upgrade

The following restrictions apply when completing an in-service software upgrade on the Cisco ASR 903 Series 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 *advipservicesk9* image to an *advipservicesk9image*) are not supported in the ISSU process.
- Running two different image types simultaneously is not supported.
- In-service upgrades from one package mode to another are not supported.
- The procedures in this document represent supported and tested installation sequences; following alternative procedures for upgrading the Cisco ASR 903 Series Router software can cause unexpected behavior.

## Single-Command Upgrade Overview

The Cisco ASR 903 Series Router supports a single-command upgrade for ISSU. A single command upgrade allows you to install a complete set of sub-packages using a single command. This command will install 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 will be 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 5-9](#).

## Downloading an Image

Follow these steps to download a Cisco ASR 903 Series Router software image.



### Caution

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

<b>Step 1</b>	Router# <b>mkdir issu</b> Create directory filename [issu]? Created dir bootflash:/issu	Creates an ISSU directory in bootflash.
<b>Step 2</b>		Download the consolidated image file from Cisco.com.
<b>Step 3</b>	Router# <b>copy filename directory</b>	Copy the consolidated image file to the ISSU bootflash directory.
	<b>Example:</b> Router# <b>copy</b> <b>asr903rsp1-adventerprisek9.upgrade.bin</b> <b>bootflash:/issu</b>	<b>Note</b> 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.

## 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 5-7](#).

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


# 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

Step 1		Download the new consolidated image file from Cisco.com. For more information about downloading Cisco software image, see <a href="#">Chapter 1, “Using Cisco IOS XE Software.”</a>
Step 2		Open a console session to the active RSP. For instructions on how to open a console session, see <a href="#">Console Port, Telnet, and SSH Handling, page 2-1.</a>
Step 3	<p>Router# <b>copy filename directory</b></p> <p><b>Example:</b>  Router# <b>copy</b>  <b>asr903rspl-adventerprisek9.upgrade.bi</b>  <b>n bootflash:/issu</b></p>	<p>Copy the new consolidated image file to the active ISSU bootflash directory such that the new image file is in the same location as the existing image file.</p> <p><b>Note</b> 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.</p> <p><b>Note</b> It is not necessary to copy the new consolidated image file to the standby RSP; the one-shot upgrade process completes this step.</p>
Step 4	Router# <b>configure terminal</b>	Enters configuration mode.
Step 5	Router(config)# <b>redundancy</b> Router(config-red)#	Enters redundancy configuration mode.
Step 6	Router(config-red)# <b>mode sso</b>	Sets the router in SSO redundancy mode.
Step 7	<p><b>end</b></p> <p><b>Example:</b>  Router(config)# <b>end</b></p>	Exits configuration mode and returns to the EXEC command prompt.
Step 8	*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 9	Router# <b>copy running-config startup-config</b>	Saves the configuration.

## Completing the Single Command Upgrade

	Command	Purpose
Step 1	<pre>request platform software package install node file file-URL [interface-module-delay delay]</pre> <p><b>Example:</b></p> <pre>Router# request platform software package install node file bootflash:/issu/asr903rsp1-adventerp risek9.upgrade.bin interface-module-delay 160</pre>	<p>Initiates the one-shot installation procedure using the consolidated image file.</p> <p><b>Note</b> You can adjust the delay between the OIR of each IM using the <b>interface-module-delay</b> keyword.</p> <p> <b>Caution</b> We recommend you set the <b>interface-module-delay</b> value to 150 seconds or greater in order to ensure sufficient time for IM software upgrades.</p> <p><b>Note</b> Keywords other than interface-module-delay are not supported.</p>
Step 2		<p>The router displays a series of STAGE/SUCCESS messages.</p> <p>For sample output of a single command upgrade, see <a href="#">Software Upgrade Examples, page 5-10</a>.</p>
Step 3	Router#	Wait for original active RSP to reboot and return to the console prompt.
Step 4		Switch to the new active console
Step 5	<pre>*Jan 12 17:52:26.516: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)</pre>	Wait for new active console to return to SSO state

## 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 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
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
=====
--- Starting standby reload ---
Finished standby reload

--- Starting wait for Standby RP to reach terminal redundancy state ---

Finished wait for Standby RP to reach terminal redundancy state

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:
  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 asr903rspl-espbases.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rspl-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rspl-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rspl-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found
asr903rspl-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rspl-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rspl-sipsps.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
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
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 ROM0UEA platform with 3670016 Kbytes of main memory

Located packages.conf
Image size 7519 inode num 38, bks cnt 2 blk size 8*512
#
Located asr903rspl-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Image size 34216240 inode num 90631, bks cnt 8354 blk size 8*512
#####
#####
#####
#####
#####
Boot 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): Chasfs initialisation 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/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto: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 903 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 9, “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
```



## CHAPTER 7

# Configuring Ethernet Interfaces

---

This chapter provides information about configuring the Gigabit Ethernet interface modules on the Cisco ASR 903 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 7-12](#)

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 the LAN-PHY Mode, page 7-12](#)

## Limitations and Restrictions

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

**REVIEW DRAFT – CISCO CONFIDENTIAL**

## 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**

	Command or Action	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# <b>interface gigabitethernet slot/subslot/port</b> or Router(config)# <b>interface tengigabitethernet slot/subslot/port</b>	Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where: <ul style="list-style-type: none"> <li>• <i>slot/subslot/port</i>—The location of the interface. See the “Specifying the Interface Address on an Interface Module” section on page 7-3.</li> </ul> <p><b>Note</b> The slot number is always 0.</p>
Step 3	Router(config-if)# <b>ip address [ip-address mask {secondary}   dhcp {client-id interface-name} {hostname host-name}]</b>	Sets a primary or secondary IP address for an interface that is using IPv4, where: <ul style="list-style-type: none"> <li>• <i>ip-address</i>—The IP address for the interface.</li> <li>• <i>mask</i>—The mask for the associated IP subnet.</li> <li>• <b>secondary</b>—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> <li>• <b>dhcp</b>—Specifies that IP addresses will be assigned dynamically using DHCP.</li> <li>• <b>client-id interface-name</b>—Specifies the client identifier. The <i>interface-name</i> sets the client identifier to the hexadecimal MAC address of the named interface.</li> <li>• <b>hostname host-name</b>—Specifies the hostname for the DHCP purposes. The <i>host-name</i> is the name of the host to be placed in the DHCP option 12 field.</li> </ul>



**REVIEW DRAFT—CISCO CONFIDENTIAL**

	Command or Action	Purpose
Step 4	Router(config-if)# <b>mtu</b> <i>bytes</i>	(As Required) Specifies the maximum packet size for an interface, where: <ul style="list-style-type: none"> <li><i>bytes</i>—The maximum number of bytes for a packet.</li> </ul> The default is 1500 bytes; the range is from 1500 to 9216.
Step 5	Router(config-if)# <b>standby</b> [ <i>group-number</i> ] <b>ip</b> [ <i>ip-address</i> [ <b>secondary</b> ]]	Creates or enables the Hot Standby Router Protocol (HSRP) group using its number and virtual IP address, where: <ul style="list-style-type: none"> <li>(Optional) <i>group-number</i>—The group number on the interface for which HSRP is being enabled. The range is from 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number.</li> <li>(Optional on all but one interface if configuring HSRP) <i>ip-address</i>—The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.</li> <li>(Optional) <b>secondary</b>—Specifies that the IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.</li> </ul> <p><b>Note</b> This command is required only for configurations that use HSRP.</p> <p><b>Note</b> This command enables HSRP but does not configure it further. For additional information on configuring HSRP, see the <a href="#">First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Release 3S</a>.</p>
Step 6	Router(config-if)# <b>no shutdown</b>	Enables the interface.

## Specifying the Interface Address on an Interface Module

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

- slot*—The chassis slot number in the Cisco ASR 903 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:

**REVIEW DRAFT – CISCO CONFIDENTIAL**

```
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).

Each router uses only three timers in HSRP. The timers time the hello messages. When a failure occurs, the HSRP converges depend on how the HSRP hello and hold timers are configured. By default, these timers are set to three and ten seconds respectively, which means that a hello packet is sent between the HSRP standby group devices every three seconds. The standby device becomes active when a hello packet is not received for ten seconds. You can lower these timer settings to speed up the failover or preemption, but, to avoid increased CPU usage and unnecessary standby state flapping, do not set the hello timer below one second or the hold timer below four seconds.

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:
UpSerial0
UpSerial1
```

**REVIEW DRAFT—CISCO CONFIDENTIAL**

## Modifying the Interface MTU Size

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  $\times$  4 bytes).

For the Gigabit Ethernet interface module on the Cisco ASR 903 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:

Command	Purpose
Router(config-if)# <b>mtu bytes</b>	Configures the maximum packet size for an interface, where: <ul style="list-style-type: none"> <li>• <i>bytes</i>—Specifies the maximum number of bytes for a packet.</li> </ul> The default is 1500 bytes and the maximum configurable MTU is 9216 bytes.

## REVIEW DRAFT – CISCO CONFIDENTIAL

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 903 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 903 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 903 Series Router, flow control is autonegotiated when autonegotiation is enabled. Autonegotiation is enabled by default.

When enabling autonegotiation, consider these guidelines:

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

**REVIEW DRAFT – CISCO CONFIDENTIAL****Enabling Autonegotiation**

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

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

**Disabling Autonegotiation**

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

Speed and duplex configurations can be advertised using autonegotiation. 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:

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

**Configuring Carrier Ethernet Features**

For information about configuring an Ethernet interface as a layer 2 Ethernet virtual circuit (EVC) or Ethernet flow point (EFP), see the [Configuring Ethernet Virtual Connections on the Cisco ASR 903 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:

Command	Purpose
Router# <b>copy running-config startup-config</b>	Writes the new configuration to NVRAM.

For information about managing your system image and configuration files, refer to the [Cisco IOS Configuration Fundamentals Configuration Guide](#) and [Cisco IOS Configuration Fundamentals Command Reference](#) publications that correspond to your Cisco IOS software release.

**REVIEW DRAFT – CISCO CONFIDENTIAL****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.

Command	Purpose
Router(config-if)# <b>shutdown</b>	Restarts, stops, or starts an interface.

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:

Command	Purpose
Router# <b>hw-module slot number</b> { <b>logging</b> } <b>reload</b> [ <b>force</b> ]   <b>start</b>   <b>stop</b> [ <b>force</b> ]	Restarts, stops, or starts a slot on the router. You can also use this command to disable or enable onboard logging of the hardware.

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

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:

Command	Purpose
Router(config-if)# <b>shutdown</b>	Disables an interface.

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

Command	Purpose
Router(config-if)# <b>no shutdown</b>	Restarts a disabled interface.

**REVIEW DRAFT – CISCO CONFIDENTIAL**

## Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 903 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 903 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
```

**REVIEW DRAFT – CISCO CONFIDENTIAL**

# 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:

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

Following are sample output of several **show** commands for SFP Modules and XFP Modules.

The following **show hw-module subslot** command sample output is for SFP-GE-S:

```
Router# show hw-module subslot 2/0 transceiver 0 idprom
IDPROM for transceiver GigabitEthernet2/0/0:
Description = SFP optics (type 3)
Transceiver Type: = GE SX (19)
Product Identifier (PID) = FTRJ8519P1BNL-C6
Vendor Revision = A
Serial Number (SN) = FNS1037R8DH
Vendor Name = CISCO-FINISAR
Vendor OUI (IEEE company ID) = 00.90.65 (36965)
CLEI code = IPUIALJRAA
Cisco part number = 10-2143-01
Device State = Enabled.
Date code (yy/mm/dd) = 06/09/14
Connector type = LC.
Encoding = 8B10B
NRZ
Nominal bitrate = GE (1300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
```

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 Identifier (PID) = FWDM-16217D49CSC
Vendor Revision = C
Serial Number (SN) = FNS10500HA9
Vendor Name = CISCO-FINISAR
```



**REVIEW DRAFT—CISCO CONFIDENTIAL**

```

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 Identifier (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

```

The following sample output is for SFP-GE-SX:

```

Router# show hw-module subslot 2/0 transceiver 0 idprom dump
IDPROM for transceiver GigabitEthernet2/0/0:
Description = SFP optics (type 3)
Transceiver Type: = GE SX (19)
Product Identifier (PID) = FTRJ8519P1BNL-C6
Vendor Revision = A
Serial Number (SN) = FNS1037R8DH
Vendor Name = CISCO-FINISAR
Vendor OUI (IEEE company ID) = 00.90.65 (36965)
CLEI code = IPUIALJRAA
Cisco part number = 10-2143-01
Device State = Enabled.
SFP IDPROM Page 0xA0:
000: 03 04 07 00 00 00 01 00 00 00
010: 00 01 0D 00 00 00 37 1B 00 00
020: 43 49 53 43 4F 2D 46 49 4E 49
030: 53 41 52 20 20 20 00 00 90 65
040: 46 54 52 4A 38 35 31 39 50 31
050: 42 4E 4C 2D 43 36 41 20 20 20
060: 03 52 00 74 00 1A 00 00 46 4E

```

**REVIEW DRAFT – CISCO CONFIDENTIAL**

```

070: 53 31 30 33 37 52 38 44 48 20
080: 20 20 20 20 30 36 30 39 31 34
090: 20 20 58 80 01
SFP IDPROM Page 0xA2:
000: 6D 00 E3 00 67 00 F3 00 98 58
010: 69 78 90 88 71 48 1D 4C 01 F4
020: 17 70 03 E8 25 19 02 F5 25 19
030: 04 A9 E3 EE 01 DF 8F C5 02 EC
040: 00 00 00 00 00 00 00 00 00 00
050: 00 00 00 00 00 00 00 00 00 00
060: 00 00 00 00 00 00 00 00 3E 5D
070: 01 79 C0 5B AC 86 01 00 00 00
080: 00 AA FF FD 01 00 00 00 01 00
090: 00 00 00 00 00 3A 1B 70 80 D8
100: 00 62 00 28 00 22 00 00 00 00
110: 82 F8 05 40 00 00 05 40 00 00
120: 00 00 00 00 00 00 00 01 49 50
130: 55 49 41 4C 4A 52 41 41 31 30
140: 2D 32 31 34 33 2D 30 31 56 30
150: 31 20 89 FB 55 00 00 00 00 78
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: AA AA 53 46 50 2D 47 45 2D 53
200: 20 20 20 20 20 20 20 20 20 20
210: 20 20 00 00 00 00 00 00 00 00
220: 00 00 00 A2 00 00 00 00 00 00
230: 00 00 00 00 00 00 00 00 00 00
240: 00 00 00 00 00 00 00 00 00 40
250: 00 40 00 00 00 00
Router#

```

## 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 the LAN-PHY Mode, page 7-12](#)
- [Configuring WAN-PHY Signal Failure and Signal Degrade Bit Error Rates, page 7-14](#)

## Configuring the LAN-PHY Mode

This section describes how to configure the 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 0/1 enable LAN**
4. **exit**
5. **show controllers wanphy interface-path-id**

**REVIEW DRAFT – CISCO CONFIDENTIAL****DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<pre>show controllers wanphy 0/1/0</pre> <p><b>Example:</b></p> <pre>Router# show controllers wanphy 0/1/0 TenGigabitEthernet0/1/0 Mode of Operation: WAN Mode SECTION   LOF = 0          LOS   = 0 BIP(B1) = 0 LINE   AIS = 0          RDI   = 0          FEBE = 0          BIP(B2) = 0 PATH   AIS = 0          RDI   = 0          FEBE = 0          BIP(B3) = 0   LOP = 0          NEWPTR = 0          PSE = 0          NSE     = 0 WIS ALARMS   SER   = 0          FELCDP = 0 FEAISP = 0   WLOS  = 0          PLCD  = 0   LFEBIP = 0         PBEC  = 0  Active Alarms[All defects]: SWLOF LAIS PAIS SER Active Alarms[Highest Alarms]: SWLOF Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA PLOP WLOS    Rx(K1/K2): 00/00  Tx(K1/K2): 00/00   S1S0 = 00, C2 = 0x1A PATH TRACE BUFFER: UNSTABLE   Remote J1 Byte :  BER thresholds:  SD = 10e-6  SF = 10e-3 TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6</pre>	<p>Displays the configuration mode of the LAN/WAN-PHY controller. By default, prior to configuration of the LAN-PHY mode, the controller operates in the WAN-PHY mode.</p>
<b>Step 2</b>	<pre>configure terminal</pre> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters the global configuration mode.</p>
<b>Step 3</b>	<pre>hw-module subslot slot/subslot enable LAN</pre> <p><b>Example:</b></p> <pre>Router(config)# hw-module subslot 0/1 enable LAN</pre>	<p>Configures the LAN PHY mode for the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter.</p>

**REVIEW DRAFT – CISCO CONFIDENTIAL**

	Command or Action	Purpose
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global-configuration (config) mode and enters privilege-exec mode.
Step 5	<b>show controllers wanphy 0/1/0</b>  <b>Example:</b> Router# show controllers wanphy 0/1/0 TenGigabitEthernet0/1/0 Mode of Operation: LAN Mode	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.

## 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.

A Signal Failure (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).

A Signal Degrade (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.

**REVIEW DRAFT – CISCO CONFIDENTIAL**

## Configuration Examples

This section includes the following configuration examples:

- [Basic Interface Configuration, page 7-15](#)
- [MTU Configuration, page 7-15](#)
- [VLAN Encapsulation, page 7-16](#)

### Basic Interface Configuration

The following example shows how to enter the global configuration mode to specify the interface that you want to configure, 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
```

### MTU Configuration

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

**Note**

---

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

---

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 0/0/1
!
! Configure the interface MTU.
!
Router(config-if)# mtu 9216
```

**REVIEW DRAFT – CISCO CONFIDENTIAL****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](#).



## CHAPTER 8

# Configuring T1/E1 Interfaces

---

This chapter provides information about configuring the T1/E1 interface module on the Cisco ASR 903 Series Router. It includes the following sections:

- [Configuration Tasks, page 8-1](#)
- [Verifying the Interface Configuration, page 8-17](#)
- [Configuration Examples, page 8-18](#)

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 903 Series Router and includes information about verifying the configuration.

It includes the following topics:

- [Required Configuration Tasks, page 8-2](#)
- [Optional Configurations, page 8-4](#)
- [Saving the Configuration, page 8-6](#)

## Limitations

This section describes the software limitations that apply when configuring the T1/E1 interface module on the Cisco ASR 903 Series Router.

The following features are not currently supported on the T1/E1 interface module:

- Serial interfaces—The Cisco ASR 903 Series Router does not currently support serial interfaces or features applied to serial interfaces. We recommend that you use a configuration with CEM or ATM IMA as a workaround.
- Channel groups—The Cisco ASR 903 Series Router does not currently support channel-groups or features applied to channel-groups. We recommend that you use a configuration with CEM or ATM IMA as a workaround.

**REVIEW DRAFT—CISCO CONFIDENTIAL**

- ATM IMA groups—You can create a maximum of 16 IMA groups on each T1/E1 interface module.
- Supported BERT patterns—Currently only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported.

## 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 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:

	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Router(config)# <b>card type {e1   t1} slot subslot</b>	Sets the serial mode for the interface module: <ul style="list-style-type: none"> <li>• <b>t1</b>—Specifies T1 connectivity of 1.536 Mbps. B8ZS is the default line code for T1.</li> <li>• <b>e1</b>—Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 1.984 Mbps in framed mode and 2.048 Mbps in unframed E1 mode.</li> <li>• <i>slot subslot</i>—Specifies the location of the interface module.</li> </ul>
<b>Step 3</b>	Router(config)# <b>exit</b>	Exits configuration mode and returns to the EXEC command interpreter prompt.



**REVIEW DRAFT—CISCO CONFIDENTIAL****Configuring the Controller**

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

	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>	Router(config)# <b>controller</b> { <b>t1</b>   <b>e1</b> } <i>slot/subslot/port</i>	<p>Selects the controller to configure and enters controller configuration mode.</p> <ul style="list-style-type: none"> <li>• <b>t1</b>—Specifies the T1 controller.</li> <li>• <b>e1</b>—Specifies the E1 controller.</li> <li>• <i>slot/subslot/port</i>—Specifies the location of the interface.</li> </ul> <p><b>Note</b> The slot number is always 0.</p>
<b>Step 2</b>	Router(config-controller)# <b>clock source</b> { <b>internal</b>   <b>line</b> }	<p>Sets the clock source.</p> <p><b>Note</b> The clock source is set to internal if the opposite end of the connection is set to line and the clock source is set to line if the opposite end of the connection is set to internal.</p> <ul style="list-style-type: none"> <li>• <b>internal</b>—Specifies that the internal clock source is used.</li> <li>• <b>line</b>—Specifies that the network clock source is used. This is the default for T1 and E1.</li> </ul>
<b>Step 3</b>	Router(config-controller)# <b>linecode</b> { <b>ami</b>   <b>b8zs</b>   <b>hdb3</b> }	<p>Selects the linecode type.</p> <ul style="list-style-type: none"> <li>• <b>ami</b>—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.</li> <li>• <b>b8zs</b>—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for T1 controller only. This is the default for T1 lines.</li> <li>• <b>hdb3</b>—Specifies high-density binary 3 (HDB3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.</li> </ul>
<b>Step 4</b>	<p><b>For T1 Controllers:</b></p> <p>Router(config-controller)# <b>framing</b> {<b>sf</b>   <b>esf</b>}</p> <p><b>For E1 Controllers:</b></p> <p>Router(config-controller)# <b>framing</b> {<b>crc4</b>   <b>no-crc4</b>}</p>	<p>Selects the framing type.</p> <ul style="list-style-type: none"> <li>• <b>sf</b>—Specifies Super Frame as the T1 frame type.</li> <li>• <b>esf</b>—Specifies Extended Super Frame as the T1 frame type. This is the default for E1.</li> <li>• <b>crc4</b>—Specifies CRC4 as the E1 frame type. This is the default for E1.</li> <li>• <b>no-crc4</b>—Specifies no CRC4 as the E1 frame type.</li> </ul>

**REVIEW DRAFT – CISCO CONFIDENTIAL**

	Command	Purpose
Step 5	<b>cablelength {long   short}</b>  <b>Example:</b> Router(config-controller)# cablelength long	To fine-tune the pulse of a signal at the receiver for an E1 cable on a Cisco AS5300 or Cisco AS5400, use the cablelength command in controller configuration mode.
Step 6	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits configuration mode and returns to the EXEC command interpreter prompt.

**Verifying Controller Configuration**

Use the **show controllers** command to verify the controller 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 Internal.
  Data in current interval (230 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
    0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Total Data (last 24 hours)
    136 Line Code Violations, 63 Path Code Violations,
    0 Slip Secs, 6 Fr Loss Secs, 4 Line Err Secs, 0 Degraded Mins,
    7 Errored Secs, 1 Bursty Err Secs, 6 Severely Err Secs, 458 Unavail Secs
    2 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

**Optional Configurations**

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

- [Configuring Framing, page 8-5](#)
- [Saving the Configuration, page 8-6](#)

**REVIEW DRAFT—CISCO CONFIDENTIAL****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
Router# <b>configure terminal</b>	Enters global configuration mode.
Router(config)# <b>controller {t1   e1}</b> <i>slot/subslot/port</i>	Selects the controller to configure. <ul style="list-style-type: none"> <li><b>t1</b>—Specifies the T1 controller.</li> <li><b>e1</b>—Specifies the E1 controller.</li> <li><i>slot/subslot/port</i>—Specifies the location of the controller.</li> </ul> <p><b>Note</b> The slot number is always 0.</p>
<b>For T1 controllers</b> Router(config-controller)# <b>framing {sf   esf}</b>	Set the framing on the interface. <ul style="list-style-type: none"> <li><b>sf</b>—Specifies Super Frame as the T1 frame type.</li> <li><b>esf</b>—Specifies Extended Super Frame as the T1 frame type. This is the default for T1.</li> </ul>
<b>For E1 controllers</b> Router(config-controller)# <b>framing {crc4   no-crc4}</b>	<ul style="list-style-type: none"> <li><b>no-crc4</b>—Specifies CRC4 frame as the E1 frame type. This is the default for E1.</li> <li><b>no-crc4</b>—Specifies no CRC4 as the E1 frame type.</li> </ul>

**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
```

**REVIEW DRAFT – CISCO CONFIDENTIAL**

## Saving the Configuration

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

Command	Purpose
Router# <b>copy running-config startup-config</b>	Writes the new configuration to NVRAM.

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

## Troubleshooting E1 and T1 Controllers

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

- [Setting Loopbacks](#)
- [Run Bit Error Rate Test](#)

### Setting Loopbacks

The following sections describe how to set loopbacks:

- [Setting a Loopback on the E1 Controller, page 8-6](#)
- [Setting a Loopback on the T1 Controller, page 8-7](#)

#### 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:

Task	Command
Select the E1 controller and enter controller configuration mode.	<b>controller e1</b> <i>slot/subslot/port</i> <b>Note</b> The slot number is always 0.
Set a diagnostic loopback on the E1 line.	<b>loopback diag</b>
Set a network payload loopback on the E1 line.	<b>loopback network</b> { <b>line</b>   <b>payload</b> }
Exit configuration mode when you have finished configuring the controller.	<b>end</b>

**REVIEW DRAFT – CISCO CONFIDENTIAL****Setting a Loopback on the T1 Controller**

To set a loopback on the T1 controller, perform the first task followed by any of the following tasks beginning in global configuration mode:

Task	Command
Select the T1 controller and enter controller configuration mode.	<b>controller t1</b> <i>slot/subslot/port</i> <b>Note</b> The slot number is always 0.
Set a diagnostic loopback on the T1 line.	<b>loopback diag</b>
Set a local loopback on the T1 line. You can select to loopback the line or the payload.	<b>loopback local</b> { <b>line</b>   <b>payload</b> }
Set 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 ESF loopback codes to communicate the request to the far end.	<b>loopback remote iboc</b>
Exit configuration mode when you have finished configuring the controller.	<b>end</b>

**Note**

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

**Table 8-1 Loopback Descriptions**

Loopback	Description
<b>loopback diag</b>	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 <b>clock source</b> command to <b>internal</b> for this loopback mode.
<b>loopback local</b>	Loops the incoming receive signal back out the transmitter. You can specify whether to use the <b>line</b> or <b>payload</b> .
<b>local line</b>	The incoming signal is looped back in the interface module using the framer's line loopback mode. The framer does not re-clock or re-frame the incoming data. All incoming data is received by the interface module's driver.
<b>local payload</b>	The incoming signal is looped back in the interface module using the framer's payload loopback mode. The framer re-clocks and re-frames the incoming data before sending it back out to the network. When in payload loopback, an all 1s data pattern is received by the local HDLC receiver, and the clock source is automatically set to line (overriding the <b>clock source</b> command). When the payload loopback is ended, the clock source returns to the last setting selected by the <b>clock source</b> command.

**REVIEW DRAFT – CISCO CONFIDENTIAL****Table 8-1 Loopback Descriptions**

<b>Loopback</b>	<b>Description</b>
<b>loopback remote iboc</b>	Attempts to set the far-end T1 interface into line loopback. This command sends an in-band bit-oriented code to the far-end to cause it to go into line loopback. This command is available when using ESF or SF framing mode.
<b>network line</b>	The incoming signal is looped back in the interface module using the framer's line loopback mode. The framer does not re-clock or re-frame the incoming data. All incoming data is received by the interface module's driver.
<b>network payload</b>	The incoming signal is looped back in the interface module using the framer's payload loopback mode. The framer re-clocks and re-frames the incoming data before sending it back out to the network. When in payload loopback, an all 1s data pattern is received by the local HDLC receiver, and the clock source is automatically set to line (overriding the <b>clock source</b> command). When the payload loopback is ended, the clock source returns to the last setting selected by the <b>clock source</b> command.

## Run Bit Error Rate Test

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 allow 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 BER 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:

<b>Task</b>	<b>Command</b>
Select the E1 or T1 controller and enter controller configuration mode.	<b>controller</b> {e1   t1} slot/subslot/port <b>Note</b> The slot number is always 0.
Specify the BERT pattern for the E1 or T1 line and the duration of the test in minutes (1 to 1440 minutes). <b>Note</b> Only the 2 <sup>11</sup> , 2 <sup>15</sup> , 2 <sup>20</sup> -O153, and 2 <sup>20</sup> -QRSS patterns are supported.	<b>bert pattern</b> {0s   1s   2 <sup>11</sup>   2 <sup>15</sup>   2 <sup>20</sup> -O153   2 <sup>20</sup> -QRSS   2 <sup>23</sup>   alt-0-1} interval minutes
Exit configuration mode when you have finished configuring the controller.	end
View the BERT results.	<b>show controllers</b> {e1   t1} slot/subslot/port

**REVIEW DRAFT—CISCO CONFIDENTIAL**

The following keywords list different BERT keywords and their descriptions.



**Caution** Currently only the 2<sup>11</sup>, 2<sup>15</sup>, 2<sup>20</sup>-O153, and 2<sup>20</sup>-QRSS patterns are supported.

**Table 8-2 BERT Pattern Descriptions**

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

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



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

You can view the results of a BER 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)

## Monitor and Maintain the T1/E1 Interface Module

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

Task	Command
Display the status of the E1 or T1 controller.	<b>show controllers {e1   t1}</b> [slot/port-adapter/port/e1-line] [brief]

**REVIEW DRAFT – CISCO CONFIDENTIAL**

Task	Command
Display statistics about the serial information for a specific E1 or T1 channel group (values are 0 to 30 for E1 and 0 to 23 for T1).	<b>show interface serial</b> <i>slot/subslot/port</i>
To clear the interface counters, use the <b>clear counters EXEC</b> command.	<b>clear counters serial</b> <i>slot/subslot/port</i>

## 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:

- [Configuring a CEM Group, page 8-10](#)
- [Using CEM Classes, page 8-11](#)
- [Configuring CEM Parameters, page 8-13](#)


**Note**

CEM is used as an element in configuring pseudowires including Structure-Agnostic TDM over Packet (SAToP) and Circuit Emulation Service over Packet-Switched Network (CESoPSN). For more information about configuring pseudowires, see [Chapter 12, “Configuring Pseudowire.”](#)

## 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**



**REVIEW DRAFT—CISCO CONFIDENTIAL**

	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
<b>Step 3</b>	<pre>controller {t1   e1} slot/subslot/port</pre> <p><b>Example:</b> Router(config)# controller t1 0/1/0</p>	Enters controller configuration mode. <ul style="list-style-type: none"> <li>• Use the slot, subslot, and port arguments to specify the slot number and port number to be configured.</li> </ul> <p><b>Note</b> The slot number is always 0.</p>
<b>Step 4</b>	<pre>cem-group group-number {unframed   timeslots timeslot}</pre> <p><b>Example:</b> Router(config-controller)# cem-group 6 timeslots 1-4,9,10 speed 64</p>	Creates a circuit emulation channel from one or more time slots of a T1 or E1 line. <ul style="list-style-type: none"> <li>• The <b>group-number</b> keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30.</li> <li>• Use the <b>unframed</b> keyword to specify that a single CEM channel is being created including all time slots and the framing structure of the line.</li> <li>• Use the <b>timeslots</b> keyword and the <i>timeslot</i> argument to specify the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.</li> </ul> <p><b>Note</b> The <b>speed</b> keyword is not currently supported.</p>
<b>Step 5</b>	<pre>end</pre> <p><b>Example:</b> Router(config-controller)# end</p>	Exits controller configuration mode and returns to privileged EXEC mode.

## Using CEM Classes

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

**Note**

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

**Note**

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

**REVIEW DRAFT – CISCO CONFIDENTIAL****SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **class cem** *classname*
4. **payload-size** *size*
5. **dejitter-buffer** *size*
6. **idle-pattern** {*pattern* | *length pattern1* [*pattern2*]}
7. **exit**
8. **interface cem** *slot/subslot/port*
9. **no ip address**
10. **cem** *slot/subslot/port*
11. **cem** *group-number*
12. **xconnect** *peer-ip-address* *vc-id* {**encapsulation** {**l2tpv3** [**manual**] | **mpls** [**manual**]} | *pw-class* *pw-class-name*} [**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]
13. **exit**
14. **exit**

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# <b>class cem</b> <b>mycemclass</b>	Creates a new CEM class
Step 4	<b>payload-size</b> <i>size</i> <b>dejitter-buffer</b> <i>size</i> <b>idle-pattern</b> { <i>pattern</i>   <i>length</i> <i>pattern1</i> [ <i>pattern2</i> ]}	Enter the configuration commands common to the CEM class. This example specifies a sample rate, payload size, dejitter buffer, and idle pattern.
Step 5	Router(config-cem-class)# <b>exit</b>	Returns to the config prompt.
Step 6	Router(config)# <b>interface cem</b> <i>0/0/0</i> Router(config-if)# <b>no ip address</b> Router(config-if)# <b>cem</b> <i>0</i> Router(config-if-cem)# <b>xconnect</b> <i>10.10.10.10</i> <i>200</i> <b>encapsulation</b> <i>mpls</i>	Configure the CEM interface that you want to use for the new CEM class. <b>Note</b> The use of the <b>xconnect</b> command can vary depending on the type of pseudowire you are configuring.

**REVIEW DRAFT – CISCO CONFIDENTIAL**

	Command	Purpose
Step 7	Router(config-if-cem) # <b>exit</b> Router(config-if) #	Exits the CEM interface.
Step 8	<b>exit</b>	Exits configuration mode.
	<b>Example:</b> Router(config) # exit Router#	

## Configuring CEM Parameters

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

- [Configuring Payload Size \(Optional\)](#), page 8-13
- [Setting the DeJitter Buffer Size](#), page 8-14
- [Setting an Idle Pattern \(Optional\)](#), page 8-14
- [Enabling Dummy Mode](#), page 8-14
- [Setting a Dummy Pattern](#), page 8-14
- [Shutting Down a CEM Channel](#), page 8-14



### 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
- 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:  $L = 8 * N * D$ . 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.

## REVIEW DRAFT – CISCO CONFIDENTIAL

### 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 500 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 8-15](#)
- [Configuring ATM IMA, page 8-15](#)

**REVIEW DRAFT – CISCO CONFIDENTIAL****Configuring a Clear-Channel ATM Interface**

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

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	Router(config)# <b>controller</b> {t1} slot/subslot/port	Selects the T1 controller for the port you are configuring (where <i>slot/subslot</i> identifies the location and <i>/port</i> identifies the port).
<b>Step 2</b>	Router(config-controller)# <b>atm</b>	Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is <i>atm/slot/subslot/port</i> . <b>Note</b> The slot number is always 0.
<b>Step 3</b>	Router(config-controller)# <b>end</b>	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.”](#)

To configure an ATM interface on the router, you must have install the ATM feature license using the license install command and enabled configuration of an ATM interface using the license feature atm command. For more information about installing licenses, see the [Software Activation Configuration Guide, Cisco IOS XE Release 3S](#).

**Note**

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

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **card type** {t1 | e1} slot [bay]
4. **controller** {t1 | e1} slot/subslot/port
5. **clock source internal**
6. **ima group** group-number

**REVIEW DRAFT—CISCO CONFIDENTIAL**

7. **exit**
8. **interface** *ATMslot/subslot/IMA group-number*
9. **no ip address**
10. **atm bandwidth dynamic**
11. **no atm ilmi-keepalive**
12. **exit**

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# <b>card type e1 0 0</b>	Specifies the slot and port number of the E1 or T1 interface.
Step 4	Router(config)# <b>controller E1 0/0/4</b> Router(config-controller)#	Specifies the controller interface on which you want to enable IMA.
Step 5	Router(config-controller)# <b>clock source internal</b>	Sets the clock source to internal.
Step 6	Router(config-controller)# <b>ima-group 0 scrambling-payload</b>	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.  <b>Note</b> This command automatically creates an ATM0/IMAx interface.
Step 7		To add another member link, repeat <a href="#">Step 3</a> to <a href="#">Step 6</a> .
Step 8	Router(config-controller)# <b>exit</b> Router(config)#	Exits the controller interface.
Step 9	<b>interface</b> <i>ATMslot/subslot/IMA group-number</i>  <b>Example:</b> Router(config-if)# <b>interface atm0/1/ima0</b>	Specify the slot location and port of IMA interface group. <ul style="list-style-type: none"> <li>• <i>slot</i>—The slot location of the ATM IMA interface module.</li> <li>• <i>group-number</i>—The group number of the IMA group.</li> </ul> The example specifies the slot number as 0 and the group number as 0.  <b>Note</b> To explicitly configure the IMA group ID for the IMA interface, you may use the optional <b>ima group-id</b> command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. At the same, the system toggles the original IMA interface to select a different IMA group ID.
Step 10	Router(config-if)# <b>no ip address</b>	Disables the IP address configuration for the physical layer interface.

**REVIEW DRAFT—CISCO CONFIDENTIAL**

	Command	Purpose
Step 11	Router(config-if)# <b>atm bandwidth dynamic</b>	Specifies the ATM bandwidth as dynamic.
Step 12	Router(config-if)# <b>no atm ilmi-keepalive</b>	Disables the Interim Local Management Interface (ILMI) keepalive parameters.
Step 13	<b>exit</b>	Exits configuration mode.
	<b>Example:</b> Router(config)# exit Router#	

**Note**

The above configuration has one IMA shorthaul with two member links (atm0/0 and atm0/1).

## Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 903 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 find detailed interface information on a per-port basis for the T1/E1 interface module, use the **show interfaces serial** command.

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

**REVIEW DRAFT – CISCO CONFIDENTIAL**

## Configuration Examples

This section includes the following configuration examples:

- Framing and Encapsulation Configuration Example, page 8-18
- CRC Configuration Example, page 8-18
- Facility Data Link Configuration Example, page 8-19
- Invert Data on the T1/E1 Interface Example, page 8-19

### Framing and Encapsulation Configuration Example

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

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller 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
```

### CRC Configuration Example

The following example sets the CRC size for the interface:

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



## REVIEW DRAFT—CISCO CONFIDENTIAL

```
! Exit global configuration mode
!
Router(config)# exit
```

### Facility Data Link Configuration Example

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
```

### Invert Data on the T1/E1 Interface Example

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
```

### CEM Configuration Example

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.”](#)

**REVIEW DRAFT – CISCO CONFIDENTIAL****Note**

---

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
```

## ATM IMA Configuration Example

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.”](#)

**Note**

---

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
```



## Configuring Clocking and Timing

---

This chapter explains how to configure timing ports on the Cisco ASR 903 Series Router RSP module.

### Clocking and Timing Overview

The Cisco ASR 903 Series Router has the following timing ports:

- 1PPS Input/Output
- 10MHz Input/Output
- ToD
- BITS

You can use the timing ports on the Cisco ASR 903 Series Router to do the following:

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



**Note**

---

Timing input and output is handled by the active RSP.

---

The following sections describe how to configure clocking and timing features on the Cisco ASR 903 Series Router.

# Timing Port Specifications

The following sections provide specifications for the timing ports on the Cisco ASR 903 Series Router.

## BITS Framing Support

Table 9-1 lists the supported framing modes for a BITS port on a Cisco ASR 903 Series Router.

**Table 9-1 Framing Modes for a BITS Port on a Cisco ASR 903 Series Router**

BITS or SSU Port Support Matrix	Framing Modes Supported	SSM or QL Support	Tx Port	Rx Port
T1	T1 ESF	Yes	Yes	Yes
T1	T1 SF	No	Yes	Yes
E1	E1 CRC4	Yes	Yes	Yes
E1	E1 FAS	No	Yes	Yes
2048 kHz	2048 kHz	No	Yes	Yes

The BITS port behaves similarly to the T1/E1 ports provided on the T1/E1 interface module; for more information about configuring T1/E1 interfaces, see [Chapter 8, “Configuring T1/E1 Interfaces.”](#)

## Clocking and Timing Restrictions

The following clocking and timing restrictions apply to the Cisco ASR 903 Series Router:

- You can configure only a single clocking input source within each group of 8 ports (0–7 and 8–15) on the T1/E1 interface module using the **network-clock input-source** command.
- PTP functionality is restricted by license type. The following table summarizes the PTP functionality available by license type:

License	PTP Support
Metro Services	Not supported
Metro IP Service	Ordinary Slave Clock
Metro Aggregation Service	Ordinary Slave Clock
Metro IP Service + IEEE 1588-2008 BC/MC	All PTP functionality including boundary and master clock
Metro Aggregation Service + IEEE 1588-2008 BC/MC	All PTP functionality including boundary and master clock



**Note**

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

# Configuring Clocking and Timing

The following sections describe how to configure clocking and timing features on the Cisco ASR 903 Series Router:

- [Configuring Input Clocking](#), page 9-3
- [Configuring Output Clocking](#), page 9-4
- [Configuring Time-of-Day Messages](#), page 9-5
- [Synchronous Ethernet ESMC and SSM](#), page 9-8
- [Configuring Calendar Updates](#), page 9-8

## Configuring Input Clocking

If you want to configure input network clocking, complete the following steps:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet *slot/subslot/port*** (gigabit ethernet interface clocking only)
4. **synchronous mode** (gigabit ethernet interface clocking only)
5. **exit** (gigabit ethernet interface clocking only)
6. **network-clock synchronization automatic**
7. **network-clock input-source *priority* {**interface** *interface\_name slot/card/port* | **ptp domain** *domain\_num* | {**external** {**R0** | **R1** [ { **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**} **line-build-out** *num* } | **e1** [**crc4** | **fas**] [**125ohm** | **75ohm**] **linecode** [**hdb3** | **ami**] } | **2m** | **10m** } }**
8. **exit**

	Command	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Router# <b>configure terminal</b>	Enter configuration mode.
Step 2	<b>interface gigabitethernet</b> <i>slot/subslot/port</i>  <b>Example:</b> Router# interface gigabitethernet 0/0/1	Enter interface configuration mode.  <b>Note</b> This step only applies if you are configuring input timing on a gigabit Ethernet interface.
Step 3	<b>synchronous mode</b>  <b>Example:</b> Router(config-if)# <b>synchronous mode</b>	Set the port in synchronous mode.  <b>Note</b> This step only applies if you are configuring input timing on a gigabit Ethernet interface.

	Command	Purpose
Step 4	Router(config-if)# <b>exit</b>	Exit interface configuration mode.  <b>Note</b> This step only applies if you are configuring input timing on a gigabit Ethernet interface.
Step 5	<b>network-clock synchronization automatic</b>  <b>Example:</b> Router(config)# [no] <b>network-clock synchronization automatic</b>	Enables G.781 based automatic clock selection process. G.781 is the ITU-T Recommendation that specifies the synchronization layer functions.
Step 6	<b>network-clock input-source</b> <i>priority</i> { <b>interface</b> <i>interface_name slot/card/port</i>   <b>ptp domain</b> <i>domain_num</i>   { <b>external</b> { <b>R0</b>   <b>R1</b> [ { <b>t1</b> { <b>sf</b>   <b>esf</b> } <b>linecode</b> { <b>ami</b>   <b>b8zs</b> } <b>line-build-out</b> <i>num</i> }   <b>e1</b> [ <b>crc4</b>   <b>fas</b> ] [ <b>125ohm</b>   <b>75ohm</b> ] <b>linecode</b> [ <b>hdb3</b>   <b>ami</b> ] }   <b>2m</b>   <b>10m</b> ] } }  <b>Example:</b> Router(config)# <b>network-clock input-source 2 external r0 e1 crc4 120ohms linecode ami</b>	Configures a clock source line interface, an external timing input interface, GPS interface, or a packet-based timing recovered clock as the input clock for the system and defines its priority. Priority is a number between 1 and 250.  This command also configures the type of signal for an external timing input interface. These signals are: <ul style="list-style-type: none"> <li>• T1 with Standard Frame format or Extended Standard Frame format.</li> <li>• E1 with or without CRC4</li> <li>• 2 MHz or 10 MHz BITS port signal. Use the R0 or R1 keyword to specify the RSP.</li> <li>• Default for Europe or Option I is e1 crc4 if the signal type is not specified.</li> <li>• Default for North America or Option II is t1 esf if signal type is not specified.</li> <li>• You can also use the <b>framing</b> argument to specify a T1 or E1 framing type.</li> </ul> <b>Note</b> The <b>no</b> version of the command reverses the command configuration, implying that the priority has changed to undefined and the state machine is informed.  <b>Note</b> You can use R0 or R1 to specify the active RSP slot.
Step 7	<b>end</b>  <b>Example:</b> Router(config)# <b>end</b>	Exit configuration mode.

## Configuring Output Clocking

If you want to configure output network clocking, complete the following steps:

### SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **network-clock synchronization automatic**
4. **network-clock output-source system** *priority* {**interface** *interface\_name slot/card/port* | **ptp domain** *domain\_num* | {**external** {**R0** | **R1** [ { **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**} **line-build-out num**} | **e1** [**crc4** | **fas**] [**125ohm** | **75ohm**] **linecode** [**hdb3** | **ami**] } | **10m** } }
5. **exit**

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enter configuration mode.
Step 2	<b>network-clock synchronization automatic</b>  <b>Example:</b> Router(config)# <b>network-clock synchronization automatic</b>	Enables G.781 based automatic clock selection process. G.781 is the ITU-T Recommendation that specifies the synchronization layer functions.
Step 3	<b>network-clock output-source system</b> <i>priority</i> { <b>interface</b> <i>interface_name slot/card/port</i>   <b>ptp domain</b> <i>domain_num</i>   { <b>external</b> { <b>R0</b>   <b>R1</b> [ { <b>t1</b> { <b>sf</b>   <b>esf</b> } <b>linecode</b> { <b>ami</b>   <b>b8zs</b> } <b>line-build-out num</b> }   <b>e1</b> [ <b>crc4</b>   <b>fas</b> ] [ <b>125ohm</b>   <b>75ohm</b> ] <b>linecode</b> [ <b>hdb3</b>   <b>ami</b> ] }   <b>10m</b> } }  <b>Example:</b> Router(config)# <b>network-clock output-source system 2 R0 2m</b>	Configures the router to transmit the system clock to external device using timing output interfaces.  <b>Note</b> You can use R0 or R1 to specify the active RSP slot.
Step 4	Router(config)# <b>end</b>	Exit configuration mode.

## Configuring Time-of-Day Messages

The Cisco ASR 903 Series Router can exchange time-of-day and 1PPS input with an external device such as a GPS receiver using the ToD and 1PPS input and output interfaces on the router.



### Caution

This feature is not currently supported.

The following sections describe how to configure time-of-day messages on the Cisco ASR 903 Series Router:

- [Configuring Input Time-of-Day Messages, page 9-6](#)
- [Configuring Output Time-of-Day Messages, page 9-7](#)

## Configuring Input Time-of-Day Messages


Use the following steps to configure input time-of-day messages:


**Note**

You can configure ToD input only on a PTP master clock port.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock domain** *domain*
4. **clock-port** *name* **master**
5. **transport ipv4** { **unicast** | **multicast** | **multicast-mix** } **interface** *interface-type interface-number* [**negotiation**]
6. **exit**
7. **tod** { **R0** | **R1** } { **iso8601** | **ubx** | **nmea** | **cisco** | **ntp** } [**delay** *delay-amount*]
8. **input** [**1pps**] { **R0** | **R1** }
9. **end**

	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	<b>ptp clock domain</b> <i>domain</i>  <b>Example:</b> Router(config)# <b>ptp clock domain</b> <i>domain</i>	Creates a Precision Time Protocol clock and specify the clock mode.  <b>Note</b> Input ToD messages are not supported on transparent or boundary clocks.
<b>Step 3</b>	Router(config-ptp-clk)# <b>clock-port</b> <i>name</i> <b>master</b>	Specifies the clocking mode of a Precision Time Protocol clock port and enters clock port configuration mode.  <b>Note</b> Input ToD messages are only supported on master clock ports.
<b>Step 4</b>	Router(config-ptp-port)# <b>transport ipv4</b> { <b>unicast</b>   <b>multicast</b>   <b>multicast-mix</b> } <b>interface</b> <i>interface-type interface-number</i> [ <b>negotiation</b> ]	Specifies the IP version, transmission mode, and interface that a Precision Time Protocol clock port uses to exchange timing packets.   <b>Caution</b> The multicast and multicast-mix modes are not currently supported.
<b>Step 5</b>	Router(config-ptp-port)# <b>exit</b>	Exits PTP clock port configuration mode.
<b>Step 6</b>	Router(config-ptp-clk)# <b>tod</b> { <b>R0</b>   <b>R1</b> } { <b>iso8601</b>   <b>ubx</b>   <b>nmea</b>   <b>cisco</b>   <b>ntp</b> } [ <b>delay</b> <i>delay-amount</i> ]	Configures the time of day message format used by the 1PPS or BITS interface.



	Command	Purpose
Step 7	Router(config-ptp-clk)# <b>input</b> [1pps] {R0   R1}	Enables Precision Time Protocol input clocking using a 1.544Mhz, 2.048Mhz, or 10Mhz timing interface or phase using the 1PPS or RS-422 interface.  Use <b>R0</b> or <b>R1</b> to specify the active RSP slot.
Step 8	Router(config)# <b>end</b>	Exit configuration mode.

## Configuring Output Time-of-Day Messages

Use the following steps to configure output time-of-day messages:



### Note

Output ToD messages are only supported on slave clock ports.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock domain** *domain*
4. **clock-port** *name slave*
5. **transport ipv4** {unicast | multicast | multicast-mix} **interface** *interface-type interface-number* [negotiation]
6. **clock source** *source-address*
7. **exit**
8. **tod** {R0 | R1} {iso8601 | ubx | nmea | cisco | ntp} [delay *delay-amount*]
9. **output 1pps** {R0 | R1} [offset *offset-value* [negative]] [*pulse-width pulse-amount* {ns | us | ms}]
10. **end**

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enter configuration mode.
Step 2	<b>ptp clock domain</b> <i>domain</i>  <b>Example:</b> Router(config)# <b>ptp clock ordinary domain 1</b>	Creates a Precision Time Protocol clock and specify the clock mode.
Step 3	<b>clock-port</b> <i>name slave</i>  <b>Example:</b> Router(config-ptp-clk)# <b>clock-port SLA slave</b>	Specifies the clocking mode of a clock port and enters clock port configuration mode.  <b>Note</b> Output ToD messages are only supported on slave clock ports.

	Command	Purpose
Step 4	<b>transport ipv4</b> {unicast   multicast   multicast-mix} <b>interface</b> <i>interface-type</i> <i>interface-number</i> [negotiation]  <b>Example:</b> Router(config-ptp-port)# <b>transport ipv4 unicast interface loopback 0 negotiation</b>	Specifies the IP version, transmission mode, and interface that a Precision Time Protocol clock port uses to exchange timing packets.
Step 5	<b>clock source</b> <i>source-address</i>  <b>Example:</b> Router(config-ptp-port)# <b>clock source 10.1.1.1</b>	Configures a connection to a Precision Time Protocol master device.
Step 6	Router(config-ptp-port)# <b>exit</b>	Exits PTP clock port configuration mode.
Step 7	<b>tod</b> {R0   R1} {iso8601   ubx   nmea   cisco   ntp} [delay <i>delay-amount</i> ]  <b>Example:</b> Router(config-ptp-clk)# <b>tod R0 ntp</b>	Configures the time of day message format used by the 1PPS or BITS interface.
Step 8	<b>output 1pps</b> {R0   R1} [offset <i>offset-value</i> [negative]] [pulse-width <i>pulse-amount</i> {ns   us   ms}]  <b>Example:</b> Router(config-ptp-clk)# <b>output 1pps R0</b>	Enables out put of time of day messages using a 1PPS interface.  Use <b>R0</b> or <b>R1</b> to specify the active RSP slot.
Step 9	Router(config)# <b>end</b>	Exit configuration mode.

## Synchronous Ethernet ESMC and SSM

The Cisco ASR 903 Series Router supports Ethernet Synchronization Message Channel (ESMC) and Synchronization Status Message (SSM) to provide clock synchronization on Synchronous Ethernet. For more information about Ethernet ESMC and SSM, see [Chapter 11, “Restoring a Clock Source.”](#)

## Configuring Calendar Updates

- To configure the router to periodically update the system calendar with PTP clock time, use the **ptp update-calendar** command.

```
Router(config)# ptp update-calendar
```



### Note

For more information about configuring clocking and timing see the [Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S](#).

# Sample Configurations

This section contains sample configurations for clocking features on the Cisco ASR 903 Series Router.

**Note**

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

**Master Clock**

```
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 negotiation
```

**Slave clock**

```
ptp clock ordinary domain 1
tod R0 ntp
output 1pps R0
clock-port SLA slave
transport ipv4 unicast interface loopback 0 negotiation
clock source 10.1.1.1
```

**Boundary clock**

```
ptp clock boundary domain 1
clock-port SLA slave
transport ipv4 unicast interface loopback 0 negotiation
clock source 10.1.1.1
clock-port master master
transport ipv4 unicast interface loopback 1 negotiation
```





# Configuring the Global Navigation Satellite System

---

**First Published: November 30, 2015**

Effective Cisco IOS-XE Release 3.17, the Cisco ASR 903 (with RSP3 module) and Cisco ASR907 routers use a satellite receiver, also called the global navigation satellite system (GNSS), as a new timing interface. With the GNSS available on the router itself, the access networks can now directly estimate time measurements and clock errors from the satellites. In other words, the Cisco ASR 903 and ASR907 routers can now act as a grandmaster clocks.

This capability simplifies network synchronization planning and provides flexibility in resolving network synchronization issues. When used in conjunction with existing synchronization networks, the GNSS capability provides a high degree of resilience.

## Information About the GNSS

- [Overview of the GNSS Module, page 10-1](#)
- [Operation of the GNSS Module, page 10-2](#)
- [Anti-Jamming, page 10-3](#)
- [High Availability for GNSS, page 10-3](#)
- [High Availability for GNSS, page 10-3](#)
- [Prerequisites for GNSS, page 10-3](#)
- [Restrictions for GNSS, page 10-3](#)

## Overview of the GNSS Module

The GNSS supports the IEEE 1588-2008 standard, which consists of a set of allowed Precision Time Protocol (PTP) features. This standard provides frequency synchronization in telecom applications.

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

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

LED Status	Description
Green	GNSS Normal State. Self survey is complete.
Amber	All other states

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

**Note**

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

## Operation of the GNSS Module

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

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

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

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

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

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

- A position relocation of the antenna of more than 100 meters is detected. This detection causes an automatic restart of the self-survey mode.
- A manual restart of the self-survey mode or when the stored reference position is deleted.
- A worst-case recovery option after a jamming-detection condition that cannot be resolved with other methods.

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

**Note**

GLONASS and BeiDou satellites cannot be enabled simultaneously.

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

- the router is reloaded when the Self-Survey mode is in progress
- the router's physical location is changed to more than 100 m from its pre-reloaded condition.

## Anti-Jamming

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

## High Availability for GNSS

The Cisco ASR 903 and Cisco ASR 907 routers have two GNSS modules, one each on the active and standby RSP3 modules. Each GNSS module must have a separate connection to the antenna in case of an RSP3 switchover.

## Prerequisites for GNSS

To use GNSS:

- 1PPS, 10 MHz, and ToD must be configured for netsync and PTP. For more information see the Configuring Clocking and Timing chapter in the *Cisco ASR 903 Router Chassis Software Configuration Guide*.
- The antenna should see as much as possible from the total sky. For proper timing, minimum of four satellites should be locked. For information, see the *Cisco ASR 903 Series Aggregation Services Router Hardware Installation Guide*.

## Restrictions for GNSS

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

## How to Configure the GNSS



### Note

To know more about the commands referenced in this document, see the [Cisco IOS Master Command List](#).

- [Enabling the GNSS License, page 10-4](#) (Required)
- [Enabling the GNSS on the Cisco Router, page 10-4](#) (Required)
- [Configuring the Satellite Constellation for GNSS, page 10-4](#) (Required)
- [Configuring Pulse Polarity and Cable Delay, page 10-4](#) (Required)
- [Configuring Cable Delay, page 10-4](#) (Required)
- [Disabling Anti-Jam Configuration, page 10-5](#) (Optional)

## Enabling the GNSS License

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

## Enabling the GNSS on the Cisco Router

```
enable
configure terminal
gnss slot ro
no shutdown
exit
```



**Note**

After the GNSS module is enabled, GNSS will be the source for 1PPS, ToD, and 10MHz clocking functions.

## Configuring the Satellite Constellation for GNSS

```
enable
configure terminal
gnss slot ro
constellation [auto | gps | galelio | beidou | qzss]
exit
```

## Configuring Pulse Polarity and Cable Delay

```
enable
configure terminal
gnss slot ro
1pps polarity negative
exit
```



**Note**

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

## Configuring Cable Delay

```
enable
configure terminal
gnss slot ro
1pps offset 5
exit
```



**Note**

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

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



## Disabling Anti-Jam Configuration

```
enable
configure terminal
gnss slot ro
anti-jam disable
exit
```

## Verifying the Configuration of the GNSS

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

```
Router# show gnss status
```

```
GNSS status:

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

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

```
Router# show gnss satellite all
```

```
All Satellites Info:
```

SV PRN No	Channel No	Acq Flg	Ephemeris Flg	SV Type	Sig Strength
14	0	1	1	0	47
21	2	1	1	0	47
22	3	1	1	0	46
18	4	1	1	0	47
27	6	1	1	0	44
31	8	1	1	0	49
24	10	1	1	0	42
79	12	0	1	1	18
78	13	1	1	1	26

```
Router# show gnss satellite 21
```

```
Selected Satellite Info:
```

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

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

## Configuration Example For Configuring GNSS

```

Router# show gns time
Current GNSS Time:

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

Router# show gns location
Current GNSS Location:

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

```

# Configuration Example For Configuring GNSS

```

gnss slot R0
no shutdown
anti-jam disable
constellation glonass
lpps polarity negative
lpps offset 1000

```

## Additional References

### Standards

Standard	Title
—	There are no associated standards for this feature.

### MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>There are no MIBs for this feature.</li> </ul>	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFC	Title
—	There are no associated RFCs for this feature.



# 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. It 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 903 Series Router.

- [Understanding Synchronous Ethernet ESMC and SSM, page 11-1](#)
- [Restrictions and Usage Guidelines, page 11-2](#)
- [Configuring Synchronous Ethernet ESMC and SSM, page 11-3](#)
- [Managing Clock Source Selection, page 11-6](#)
- [Sample Configurations, page 11-11](#)

## 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 903 Series Router synchronizes to the best available clock source. If no better clock sources are available, the router remains synchronized to the current clock source.

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



**Note**

---

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

---

## Clock Selection Modes

The Cisco ASR 903 Series Router supports two clock selection modes, which are described in the following sections.

### QL-Enabled Mode

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

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

### QL-Disabled Mode

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

- Clock availability
- Priority

**Note**

---

You can use override the default clock selection using the commands described in the [“Managing Clock Source Selection”](#) section on page 11-6.

---

## Managing Clock Selection

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

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

For more information about how to use these features, see [Managing Clock Source Selection, page 11-6](#).

## Restrictions and Usage Guidelines

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

- To use the **network-clock synchronization ssm option** command, ensure that the router configuration does not include the following:
  - Input clock source
  - Network clock quality level

- Network clock source quality source (synchronous Ethernet interfaces)
- The **network-clock synchronization ssm option** command must be compatible with the **network-clock eec** command in the configuration.
- To use the **network-clock synchronization ssm option** command, ensure that there is not a network clocking configuration applied to synchronous Ethernet interfaces, BITS interfaces, and timing port interfaces.
- SSM and ESMC are SSO-coexistent, but not SSO-compliant. The router goes into hold-over mode during switchover and restarts clock selection when the switchover is complete.
- It is recommended that you do not configure multiple input sources with the same priority as this impacts the  $T_{SM}$  (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.

## Configuring Synchronous Ethernet ESMC and SSM

Follow these steps to configure ESMC and SSM on the Cisco ASR 903 Series Router.

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>network-clock synchronization automatic</b>  <b>Example:</b> Router(config)# 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.
Step 4	<b>network-clock eec {1   2}</b>  <b>Example:</b> Router(config)# network-clock eec 1	Specifies the Ethernet Equipment Clock (EEC) type. Valid values are <ul style="list-style-type: none"> <li>• 1—ITU-T G.8262 option 1 (2048)</li> <li>• 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544)</li> </ul>

	Command or Action	Purpose
Step 5	<p><b>network-clock synchronization ssm option</b> {1   2 {GEN1   GEN2}}</p> <p><b>Example:</b> Router(config)# network-clock synchronization ssm option 2 GEN2</p>	<p>Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command:</p> <ul style="list-style-type: none"> <li>Option 1 refers to G.781 synchronization option 1, which is designed for Europe. This is the default value.</li> <li>Option 2 refers to G.781 synchronization option 2, which is designed for the United States.</li> <li>GEN1 specifies option 2 Generation 1 synchronization.</li> <li>GEN2 specifies option 2 Generation 2 synchronization.</li> </ul>
Step 6	<p><b>network-clock input-source priority</b> {<b>interface</b> <i>interface_name slot/card/port</i>   <b>ptp domain</b> <i>domain_num</i>   {<b>external</b> {R0   R1 [ { t1 {sf   esf } linecode {ami   b8zs} line-build-out <i>length</i> }   e1 [crc4   fas] [125ohm   75ohm] linecode [hdb3   ami] }   2m   10m } }</p> <p><b>Example:</b> Router(config)# network-clock input-source 1 interface GigabitEthernet 0/0/1</p>	<p>Enables you to select an interface as an input clock for the router. You can select the BITS, Gigabit Ethernet 0/0, Gigabit Ethernet 0/1 interfaces, or GPS interfaces, or an external interface.</p>
Step 7	<p><b>network-clock synchronization mode ql-enabled</b></p> <p><b>Example:</b> Router(config)# network-clock synchronization mode ql-enabled</p>	<p>Enables automatic selection of a clock source based on quality level (QL).</p> <p><b>Note</b> This command is disabled by default.</p>
Step 8	<p><b>network-clock hold-off</b> {0   <i>milliseconds</i>}</p> <p><b>Example:</b> Router(config)# network-clock hold-off 0</p>	<p>(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.</p> <p><b>Note</b> You can also specify a hold-off value for an individual interface using the <b>network-clock hold-off</b> command in interface mode.</p>
Step 9	<p><b>network-clock wait-to-restore</b> <i>seconds</i></p> <p><b>Example:</b> Router(config)# network-clock wait-to-restore 70</p>	<p>(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.</p> <p>Valid values are 0 to 86400 seconds. The default value is 300 seconds.</p> <p><b>Note</b> You can also specify a wait-to-restore value for an individual interface using the <b>network-clock wait-to-restore</b> command in interface mode.</p>
Step 10	<p><b>network-clock revertive</b></p> <p><b>Example:</b> Router(config)# network-clock revertive</p>	<p>(Optional) Sets the router in revertive switching mode when recovering from a failure. Do disable revertive mode, use the <b>no</b> form of this command.</p>

	Command or Action	Purpose
Step 11	<b>esmc process</b>  <b>Example:</b> Router(config)# esmc process	Enables the ESMC process globally.
Step 12	<b>network-clock external slot/card/port hold-off {0   milliseconds}</b>  <b>Example:</b> Router(config)# network-clock external 0/1/0 hold-off 0	Overrides the hold-off timer value for the external interface.
Step 13	<b>network-clock quality-level {tx   rx} value {interface interface-name slot/card/port   controller [E1   BITS] slot/card/port   external [2m   10m] }</b>  <b>Example:</b> Router(config)# network-clock quality-level rx qL-pRC external R0 e1 cas crc4	Specifies a quality level for a line or external clock source. The available quality values depend on the G.781 synchronization settings specified by the <b>network-clock synchronization ssm option</b> command: <ul style="list-style-type: none"> <li>• Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.</li> <li>• Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.</li> <li>• Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.</li> </ul>
Step 14	<b>interface type number</b>  <b>Example:</b> Router(config)# interface GigabitEthernet 0/0/1 Router(config-if)#	Enters interface configuration mode.
Step 15	<b>synchronous mode</b>  <b>Example:</b> Router(config-if)# synchronous mode	Configures the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface.
Step 16	<b>esmc mode [ql-disabled   tx   rx] value</b>  <b>Example:</b> Router(config-if)# esmc mode rx QL-STU	Enables the ESMC process at the interface level. The <b>no</b> form of the command disables the ESMC process.
Step 17	<b>network-clock hold-off {0   milliseconds}</b>  <b>Example:</b> Router(config-if)# network-clock hold-off 0	(Optional) Configures an interface-specific hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.  You can configure the hold-off time to either 0 or any value between 50 to 10000 ms. The default value is 300 ms.

	Command or Action	Purpose
Step 18	<b>network-clock wait-to-restore</b> <i>seconds</i>  <b>Example:</b> Router(config-if)# network-clock wait-to-restore 70	(Optional) Configures wait-to-restore timer for an individual synchronous Ethernet interface.
Step 19	<b>end</b>  <b>Example:</b> Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

You can use the **show network-locks** command to verify your configuration.

## Managing Clock Source Selection

The following sections describe how to manage the selection on the Cisco ASR 903 Series Router:

- [Specifying a Clock Source, page 11-6](#)
- [Disabling a Clock Source, page 11-8](#)

### 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 11-6](#)
- [Forcing a Clock Source Selection, page 11-7](#)
- [Disabling Clock Source Specification Commands, page 11-8](#)

### 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.



Command	Purpose
<b>network-clock switch manual external R0   R1 {{E1 {crc4   cas  fas}} {T1 {d4   sf   esf}} }</b>  <b>Example:</b> Router# <b>network-clock switch manual external r0 e1 crc4</b>	Manually selects a synchronization source, provided the source is available and is within the range.
<b>network-clock clear switch {t0   external slot/card/port [10m   2m]}</b>  <b>Example:</b> Router# network-clock clear switch t0	Disable a clock source selection.

## 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**.

Command	Purpose
<b>network-clock switch force external R0   R1 {{E1 {crc4   cas  fas}} {T1 {d4   sf   esf}} }</b>  <b>Example:</b> Router# <b>network-clock switch force r0 e1 crc4</b>	Forces the router to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.
<b>network-clock clear switch {t0   external slot/card/port [10m   2m]}</b>  <b>Example:</b> Router# network-clock clear switch t0	Disable a clock source selection.

## 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.

Command	Purpose
<b>network-clock clear switch</b> {t0   external slot/card/port [10m   2m]}  <b>Example:</b> Router# <b>network-clock clear switch t0</b>	Disable a clock source selection.

## 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 11-8](#)
- [Restoring a Clock Source, page 11-9](#)

## 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
<b>network-clock set lockout</b> {interface interface_name slot/card/port   external {R0   R1 [ { t1 {sf   esf } linecode {ami   b8zs} }   e1 [crc4   fas] linecode [hdb3   ami]} }  <b>Example:</b> Router# <b>network-clock set lockout interface GigabitEthernet 0/0/0</b>	Prevents the router from selecting a specific synchronous Ethernet clock source.
<b>network-clock clear lockout</b> {interface interface_name slot/card/port   external {R0   R1 [ { t1 {sf   esf } linecode {ami   b8zs} }   e1 [crc4   fas] linecode [hdb3   ami] } }  <b>Example:</b> Router# <b>network-clock clear lockout interface GigabitEthernet 0/0/0</b>	Disable a lockout configuration on a synchronous Ethernet clock source.

## 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
<b>network-clock clear lockout</b> { <b>interface</b> <i>interface_name</i> <i>slot/card/port</i>   <b>external external</b> { <b>R0</b>   <b>R1</b> [ { <b>t1</b> { <b>sf</b>   <b>esf</b> } <b>linecode</b> { <b>ami</b>   <b>b8zs</b> } }   <b>e1</b> [ <b>crc4</b>   <b>fas</b> ] <b>linecode</b> [ <b>hdb3</b>   <b>ami</b> ] }  <b>Example:</b>  Router# <b>network-clock clear</b> <b>lockout interface GigabitEthernet</b> <b>0/0/0</b>	Forces the router to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.

## Verifying the Configuration

You can use the following commands to verify your configuration:

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

## Troubleshooting

Table 11-1 list the debug commands that are available for troubleshooting the SyncE configuration on the Cisco ASR 903 Series Router:



### Caution

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

**Table 11-1** SyncE Debug Commands

Debug Command	Purpose
<code>debug platform network-clock</code>	Debugs issues related to the network clock, such as alarms, OOR, active-standby sources not selected correctly, and so on.

**Table 11-1** SyncE Debug Commands (continued)

Debug Command	Purpose
<code>debug network-clock</code>	Debugs issues related to network clock selection.
<code>debug esmc error</code> <code>debug esmc event</code> <code>debug esmc packet [interface &lt;interface name&gt;]</code> <code>debug esmc packet rx [interface &lt;interface name&gt;]</code> <code>debug esmc packet tx [interface &lt;interface name&gt;]</code>	Verify whether the ESMC packets are transmitted and received with proper quality-level values.

Table 11-2 provides the information about troubleshooting your configuration

**Table 11-2** Troubleshooting Scenarios

Problem	Solution
<b>Clock selection</b>	<ul style="list-style-type: none"> <li>Verify that there are no alarms on the interfaces using the <b>show network-clock synchronization detail</b> command.</li> <li>Ensure that the nonrevertive configurations are in place.</li> <li>Reproduce the issue and collect the logs using the <b>debug network-clock errors</b>, <b>debug network-clock event</b>, and <b>debug network-clock sm</b> commands. Contact Cisco Technical Support if the issue persists.</li> </ul>
<b>Incorrect QL values</b>	<ul style="list-style-type: none"> <li>Ensure that there is no framing mismatch with the SSM option.</li> <li>Reproduce the issue using the <b>debug network-clock errors</b> and <b>debug network-clock event</b> commands.</li> </ul>
<b>Alarms</b>	<ul style="list-style-type: none"> <li>Reproduce the issue using the <b>debug platform network-clock</b> command enabled in the RSP. Alternatively, enable the <b>debug network-clock event</b> and <b>debug network-clock errors</b> commands.</li> </ul>
<b>Incorrect clock limit set or queue limit disabled mode</b>	<ul style="list-style-type: none"> <li>Verify that there are no alarms on the interfaces using the <b>show network-clock synchronization detail</b> command.</li> <li>Use the <b>show network-clock synchronization</b> command to confirm if the system is in revertive mode or nonrevertive mode and verify the non-revertive configurations.</li> <li>Reproduce the current issue and collect the logs using the <b>debug network-clock errors</b>, <b>debug network-clock event</b>, and <b>debug network-clock sm</b> RSP commands.</li> </ul>
<b>Incorrect QL values when you use the show network-clock synchronization detail command.</b>	<ul style="list-style-type: none"> <li>Use the <b>network clock synchronization SSM (option 1   option 2)</b> command to confirm that there is no framing mismatch. Use the <b>show run interface</b> command to validate the framing for a specific interface. For the SSM option 1, framing should be SDH or E1, and for SSM option 2, it should be T1.</li> <li>Reproduce the issue using the <b>debug network-clock errors</b> and <b>debug network-clock event</b> RSP commands.</li> </ul>

# Sample Configurations

## Input Synchronous Ethernet Clocking

The following example configures 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
```





## CHAPTER 12

# Configuring Pseudowire

---

This chapter provides information about configuring pseudowire 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 12-9](#)
- [Configuring Circuit Emulation Service over Packet-Switched Network \(CESoPSN\), page 12-10](#)
- [Configuring an ATM over MPLS Pseudowire, page 12-12](#)
- [Configuring an Ethernet over MPLS Pseudowire, page 12-17](#)
- [Configuring Pseudowire Redundancy, page 12-19](#)
- [Verifying the Interface Configuration, page 12-21](#)
- [Sample Configurations, page 12-22](#)

## 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 and Circuit Emulation Service over Packet-Switched Network. The following sections provide an overview of these pseudowire types.

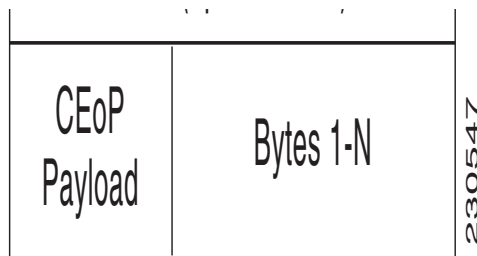
### Structure-Agnostic TDM over Packet

SAToP encapsulates TDM bit-streams (T1, E1, T3, E3) as PWs over PSNs. 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 PEs. For example, a T1 attachment circuit is treated the same way for all delivery methods, including: PE on copper, multiplex in a T3 circuit, mapped into a virtual tributary of a SONET/SDH circuit, or carried over a network using unstructured Circuit Emulation Service (CES). Termination of specific carrier layers used between the PE and circuit emulation (CE) is performed by an appropriate network service provider (NSP).

In the 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 Mode Frame Format**



[Table 12-1](#) shows the payload and jitter limits for the T1 lines in the SAToP frame format.

**Table 12-1 SAToP T1 Frame: Payload and Jitter Limits**

Maximum Payload	Maximum Jitter	Minimum Jitter	Minimum Payload	Maximum Jitter	Minimum Jitter
960	320	10	192	64	2

[Table 12-2](#) shows the payload and jitter limits for the E1 lines in the SAToP frame format.

**Table 12-2 SAToP E1 Frame: Payload and Jitter Limits**

Maximum Payload	Maximum Jitter	Minimum Jitter	Minimum Payload	Maximum Jitter	Minimum Jitter
1280	320	10	256	64	2

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

## Circuit Emulation Service over Packet-Switched Network

CESoPSN encapsulates structured (NxDS0) 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 NxDS0 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 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 Mode Frame Format**

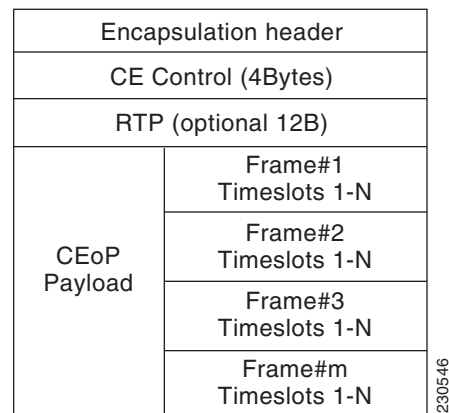


Table 12-3 shows the payload and jitter for the DS0 lines in the CESoPSN mode.

**Table 12-3 CESoPSN DS0 Lines: Payload and Jitter Limits**

DS0	Maximum Payload	Maximum Jitter	Minimum Jitter	Minimum Payload	Maximum Jitter	Minimum Jitter
1	40	320	10	32	256	8
2	80	320	10	32	128	4
3	120	320	10	33	128	4
4	160	320	10	32	64	2
5	200	320	10	40	64	2
6	240	320	10	48	64	2
7	280	320	10	56	64	2
8	320	320	10	64	64	2
9	360	320	10	72	64	2
10	400	320	10	80	64	2
11	440	320	10	88	64	2
12	480	320	10	96	64	2
13	520	320	10	104	64	2
14	560	320	10	112	64	2

DS0	Maximum Payload	Maximum Jitter	Minimum Jitter	Minimum Payload	Maximum Jitter	Minimum Jitter
15	600	320	10	120	64	2
16	640	320	10	128	64	2
17	680	320	10	136	64	2
18	720	320	10	144	64	2
19	760	320	10	152	64	2
20	800	320	10	160	64	2
21	840	320	10	168	64	2
22	880	320	10	176	64	2
23	920	320	10	184	64	2
24	960	320	10	192	64	2
25	1000	320	10	200	64	2
26	1040	320	10	208	64	2
27	1080	320	10	216	64	2
28	1120	320	10	224	64	2
29	1160	320	10	232	64	2
30	1200	320	10	240	64	2
31	1240	320	10	248	64	2
32	1280	320	10	256	64	2

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

## Transportation of Service Using ATM over MPLS

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

You can configure ATM over MPLS in the following modes:

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

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



### Note

Release 15.1(1)MR does not support ATM over MPLS N-to-1 Cell Mode or 1-to-1 Cell Mode.

For more information about how to configure ATM over MPLS, see [Configuring an ATM over MPLS Pseudowire](#).

## 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 12-17](#).

## 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 12-5](#)
- [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**

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>controller</b> {t1   e1} <i>slot/subslot/port</i>  <b>Example:</b> Router(config)# controller t1 1/0	Enters controller configuration mode. <ul style="list-style-type: none"> <li>• Use the slot and port arguments to specify the slot number and port number to be configured.</li> </ul> <b>Note</b> The slot number is always 0.
Step 4	<b>cem-group</b> <i>group-number</i> { <b>unframed</b>   <b>timeslots</b> <i>timeslot</i> }  <b>Example:</b> Router(config-controller)# cem-group 6 timeslots 1-4,9,10	Creates a circuit emulation channel from one or more time slots of a T1 or E1 line. <ul style="list-style-type: none"> <li>• The <b>group-number</b> keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30.</li> <li>• Use the <b>unframed</b> keyword to specify that a single CEM channel is being created including all time slots and the framing structure of the line.</li> <li>• Use the <b>timeslots</b> keyword and the <i>timeslot</i> argument to specify the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.</li> </ul>
Step 5	<b>end</b>  <b>Example:</b> Router(config-controller)# end	Exits controller configuration mode and returns to privileged EXEC mode.

## Using CEM Classes

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



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



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

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# <b>class cem mycemclass</b>	Creates a new CEM class
Step 4	Router(config-cem-class)# <b>payload-size 512</b> Router(config-cem-class)# <b>de jitter-buffer 10</b> Router(config-cem-class)# <b>idle-pattern 0x55</b>	Enter the configuration commands common to the CEM class. This example specifies a sample rate, payload size, dejitter buffer, and idle pattern.
Step 5	Router(config-cem-class)# <b>exit</b>	Returns to the config prompt.
Step 6	Router(config)# <b>interface cem 0/0</b> Router(config-if)# <b>no ip address</b> Router(config-if)# <b>cem 0</b> Router(config-if-cem)# <b>cem class mycemclass</b> Router(config-if-cem)# <b>xconnect 10.10.10.10 200 encapsulation mpls</b>	Configure the CEM interface that you want to use for the new CEM class. <b>Note</b> The use of the <b>xconnect</b> command can vary depending on the type of pseudowire you are configuring.
Step 7	Router(config-if-cem)# <b>exit</b> Router(config-if)#	Exits the CEM interface.
Step 8	<b>exit</b>  <b>Example:</b> Router(config)# exit Router#	Exits configuration mode.

## 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 12-8
- [Setting an Idle Pattern \(Optional\)](#), page 12-8
- [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
- 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:  $L = 8 * N * D$ . 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  $16 * DS0$  has a default payload size of 128 bytes.

The payload size must be an integer 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 500 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 Structure-Agnostic TDM over Packet (SAToP)

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

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	<b>controller</b> [T1 E1] 0/4  <b>Example:</b> Router(config-controller)# controller t1	Configures the T1 or E1 interface.
Step 4	<b>cem-group</b> <b>group-number</b> { <b>unframed</b>   <b>timeslots</b> <i>timeslot</i> }  <b>Example:</b> Router(config-if)# <b>cem-group</b> 4 <b>unframed</b>	Assigns channels on the T1 or E1 circuit to the CEM channel. This example uses the <b>unframed</b> parameter to assign all the T1 timeslots to the CEM channel.
Step 5	Router(config)# <b>interface</b> CEM0/4 Router(config-if)# <b>no ip address</b> Router(config-if)# <b>cem</b> 4	Defines a CEM group.

	Command	Purpose
Step 6	Router(config-if)# <b>xconnect</b> 30.30.30.2 304 <b>encapsulation mpls</b>	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.
Step 7	<b>exit</b>	Exits configuration mode.
	<b>Example:</b> Router(config)# <b>exit</b> Router#	

**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)

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

	Command	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
	<b>Example:</b> Router> <b>enable</b>	
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# <b>configure terminal</b>	
Step 3	Router(config)# <b>controller [e1 t1]</b> 0/0 Router(config-controller)#	Enters configuration mode for the E1 or T1 controller.
Step 4	Router(config-controller)# <b>cem-group 5 timeslots 1-24</b>	Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the <b>timeslots</b> parameter to assign specific timeslots to the CEM channel.
Step 5	Router(config-controller)# <b>exit</b> Router(config)#	Exits controller configuration.
Step 6	Router(config)# <b>interface CEM0/5</b> Router(config-if-cem)# <b>cem 5</b>	Defines a CEM channel.



	Command	Purpose
Step 7	Router(config-if-cem)# <b>xconnect</b> 30.30.30.2 305 <b>encapsulation mpls</b>	Binds an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 5 to the remote peer 30.30.30.2.  <b>Note</b> 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 <b>ip route 30.30.30.2 255.255.255.255 1.2.3.4</b> .
Step 8	Router(config-if-cem)# <b>exit</b> Router(config)#	Exits the CEM interface.
Step 9	<b>exit</b>	Exits configuration mode.
	<b>Example:</b> Router(config)# exit Router#	

## Configuring a Clear-Channel ATM Pseudowire

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

	Command or Action	Purpose
Step 1	Router(config)# <b>controller</b> {t1} <i>slot/subslot/port</i>	Selects the T1 controller for the port you are configuring.  <b>Note</b> The slot number is always 0.
Step 2	Router(config-controller)# <b>atm</b>	Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is <i>atm/slot/subslot/port</i> .  <b>Note</b> The slot number is always 0.
Step 3	Router(config-controller)# <b>exit</b>	Returns you to global configuration mode.
Step 4	Router(config)# <b>interface</b> <i>atm/slot/subslot/port</i>	Selects the ATM interface in Step 2.
Step 5	Router(config-if)# <b>pvc</b> <i>vpi/vci</i>	Configures a PVC for the interface and assigns the PVC a VPI and VCI. Do not specify 0 for both the VPI and VCI.
Step 6	Router(config-if)# <b>xconnect</b> <i>peer-router-id vcid</i> { <b>encapsulation mpls</b>   <b>pseudowire-class name</b> }	Configures a pseudowire to carry data from the clear-channel ATM interface over the MPLS network.
Step 7	Router(config-if)# <b>end</b>	Exits configuration mode.

# 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.

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# <b>card type e1 0 0</b>	Configures IMA on an E1 or T1 interface.
Step 4	Router(config)# <b>controller E1 0/4</b> Router(config-controller)#	Specifies the controller interface on which you want to enable IMA.
Step 5	Router(config-controller)# <b>clock source internal</b>	Sets the clock source to internal.
Step 6	Router(config-controller)# <b>ima-group 0 scrambling-payload</b>	If you want to configure an ATM IMA backhaul, use the <b>ima-group</b> command to assign the interface to an IMA group. For a T1 connection, use the <b>no-scrambling-payload</b> to disable ATM-IMA cell payload scrambling; for an E1 connection, use the <b>scrambling-payload</b> parameter to enable ATM-IMA cell payload scrambling.  The example assigns the interface to IMA group 0 and enables payload scrambling.
Step 7	<b>exit</b>  <b>Example:</b> Router(config)# exit Router#	Exits configuration mode.

**Note**

For more information about configuring IMA groups, see the “[Configuring ATM IMA](#)” section on page 8-15.

## 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.

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config-controller)# <b>interface ATMslot/IMAgroup-number</b>  <b>Example:</b> Router(config-controller)# <b>interface atm0/ima0</b> Router(config-if)#	Specifies the slot location and port of IMA interface group. The syntax is as follows: <ul style="list-style-type: none"> <li><i>slot</i>—The slot location of the interface module.</li> <li><i>group-number</i>—The group number of the IMA group.</li> </ul> <p>The example specifies the slot number as 0 and the group number as 0.</p> <p><b>Note</b> To explicitly configure the IMA group ID for the IMA interface, you may use the optional <b>ima group-id</b> command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. At the same, the system toggles the original IMA interface to select a different IMA group ID.</p>
Step 4	Router(config-if)# <b>no ip address</b>	Disables the IP address configuration for the physical layer interface.
Step 5	Router(config-if)# <b>atm bandwidth dynamic</b>	Specifies the ATM bandwidth as dynamic.

	Command	Purpose
Step 6	Router(config-if)# <b>no atm ilmi-keepalive</b>	Disables the ILMI keepalive parameters.
Step 7	<b>exit</b>	Exits configuration mode.
	<b>Example:</b> Router(config)# exit Router#	

For more information about configuring IMA groups, see the [“Configuring ATM IMA” section on page 8-15](#).

## Configuring the ATM over MPLS Pseudowire Interface

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

- [Configuring N-to-1 VCC Cell Transport Pseudowire](#)—Maps multiple VCCs to a single pseudowire
- [Configuring N-to-1 VPC Cell Transport](#)—Maps multiple VPCs to a single pseudowire
- [Configuring ATM AAL5 SDU VCC Transport](#)—Maps a single ATM PVC to another ATM PVC
- [Optional Configurations](#)—Maps one physical port to a single pseudowire connection
- [Optional Configurations](#)



### Note

Release 15.1(1)MR does not support N-to-1 VCC Cell Transport for mapping multiple PVCs, 1-to-1 VCC Cell Mode, or PVC mapping.



### Note

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

## 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. Follow these steps to configure an N-to-1 pseudowire.

You can use the following methods to configure an N-to-1 VCC Cell Transport pseudowire.

### Mapping a Single PVC to a Pseudowire

To map a single PVC to an ATM over MPLS pseudowire, apply the **xconnect** command at the PVC level. This configuration type only uses AAL0 encapsulation. Follow 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.

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# <b>interface atm0/ima0</b>	Configures the ATM IMA interface.
Step 4	Router(config-if)# <b>pvc 0/40</b> <b>l2transport</b> Router(cfg-if-atm-l2trans-pvc)#	Defines a PVC. Use the <b>l2transport</b> keyword to configure the PVC as layer 2 virtual circuit.
Step 5	Router(cfg-if-atm-l2trans-pvc)# <b>encapsulation aal0</b>	Defines the encapsulation type for the PVC.
Step 6	Router(config-if)# <b>xconnect 1.1.1.1</b> <b>40 encapsulation mpls</b> Router(cfg-if-atm-l2trans-pvc-xconn)#	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(cfg-if-atm-l2trans-pvc-xconn)# <b>end</b> Router#	Exits configuration mode.

## Configuring N-to-1 VPC Cell Transport

An N-to-1 VPC cell transport pseudowire maps one or more ATM virtual path connections (VPCs) to a single pseudowire. While the configuration is similar to one-to-one VPC cell mode, this transport method uses the N-to-1 VPC Pseudowire protocol and format defined in RFCs 4717 and 4446. Follow these steps to configure an N-to-1 VPC pseudowire.



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

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# <b>interface atm0/ima0</b> Router(config-if)#	Configures the ATM IMA interface.

	Command	Purpose
Step 4	Router(config-if)# <b>atm pvp 10</b> <b>l2transport</b> Router(cfg-if-atm-l2trans-pvp)#	Maps a PVP to a pseudowire
Step 5	Router(cfg-if-atm-l2trans-pvp)# <b>xconnect 30.30.30.2 305 encapsulation</b> <b>mpls</b> Router(cfg-if-atm-l2trans-pvp-xconn)#	Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 305 to the remote peer 30.30.30.2.
Step 6	Router(cfg-if-atm-l2trans-pvp-xconn)# <b>end</b> Router#	Exits configuration mode.

## Configuring ATM AAL5 SDU VCC Transport

An ATM AAL5 SDU VCC transport pseudowire maps a single ATM PVC to another ATM PVC. Follow these steps to configure an ATM AAL5 SDU VCC transport pseudowire.

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# interface atm 0/ima0 Router(config-if)#	Configures the ATM IMA interface.
Step 4	Router(config-if)# <b>pvc 0/12</b> <b>l2transport</b> Router(cfg-if-atm-l2trans-pvc)#	Configures a PVC and specify a VCI/VPI.
Step 5	Router(cfg-if-atm-l2trans-pvc)# <b>encapsulation aal5</b>	Sets the PVC encapsulation type to AAL5. <b>Note</b> You must use AAL5 encapsulation for this transport type.
Step 6	Router(cfg-if-atm-l2trans-pvc)# <b>xconnect 25.25.25.25 125</b> <b>encapsulation mpls</b>	Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 125 to the remote peer 25.25.25.25.
Step 7	<b>exit</b>  <b>Example:</b> Router(config)# exit Router#	Exits configuration mode.

## 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.

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	Router(config)# <b>int atm1/0</b>	Configures the ATM interface.
Step 4	Router(config)# <b>int atm1/0</b> Router(config-if)# <b>atm mcpt-timers</b> <b>1000 2000 3000</b>	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.
Step 5	Router(config)# <b>pvc 0/11</b> <b>l2transport</b> Router(cfg-if-atm-l2trans-pvc)# <b>encapsulation aal0</b> Router(cfg-if-atm-l2trans-pvc)# <b>cell-packing 20 mcpt-timer 3</b>	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.
Step 6	<b>end</b>  <b>Example:</b> Router(cfg-if-atm-l2trans-pvc)# <b>end</b> Router#	Exits configuration mode.

## 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.

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface interface-id</b>  <b>Example:</b> Router(config)# <b>interface</b> <b>gigabitethernet 0/0/4</b>	Specifies the port on which to create the pseudowire and enters interface configuration mode. Valid interfaces are physical Ethernet ports.
Step 4	<b>service instance number ethernet</b> <b>[name]</b>  <b>Example:</b> Router(config-if)# <b>service instance</b> <b>2 ethernet</b>	Configure an EFP (service instance) and enter service instance configuration mode. <ul style="list-style-type: none"> <li>The <i>number</i> is the EFP identifier, an integer from 1 to 4000.</li> <li>(Optional) <b>ethernet name</b> is the name of a previously configured EVC. You do not need to use an EVC name in a service instance.</li> </ul> <b>Note</b> You can use service instance settings such as encapsulation, dot1q, and rewrite to configure tagging properties for a specific traffic flow within a given pseudowire session. For more information, see <a href="#">Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router</a> .
Step 5	<b>encapsulation {default   dot1q  </b> <b>priority-tagged   untagged}</b>  <b>Example:</b> Router (config-if-srv)# <b>encapsulation dot1q 2</b>	Configure encapsulation type for the service instance. <ul style="list-style-type: none"> <li><b>default</b>—Configure to match all unmatched packets.</li> <li><b>dot1q</b>—Configure 802.1Q encapsulation.</li> <li><b>priority-tagged</b>—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7.</li> <li><b>untagged</b>—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation.</li> </ul>



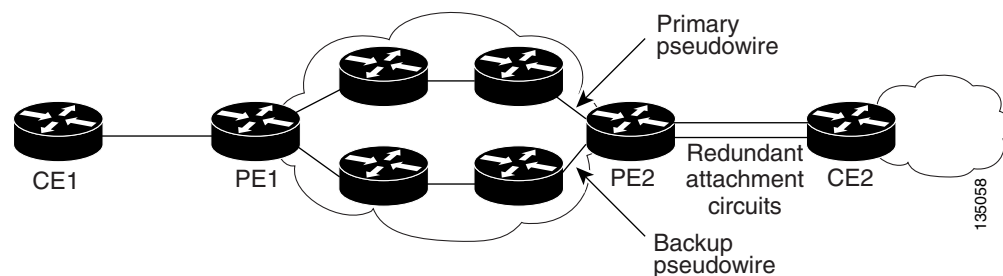
	Command	Purpose
Step 6	<pre>xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual]   mpls [manual]}   pw-class pw-class-name }[pw-class pw-class-name] [sequencing {transmit   receive   both}]</pre> <p><b>Example:</b> Router (config-if-srv)# <b>xconnect</b> <b>10.1.1.2 101 encapsulation mpls</b></p>	<p>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.</p> <p><b>Note</b> 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 <b>ip route 10.30.30.2 255.255.255.255 10.2.3.4</b>.</p>
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(config)# <b>exit</b> Router#</p>	Exits configuration mode.

## 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**



**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:

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	<b>pseudowire-class</b> [ <i>pw-class-name</i> ]  <b>Example:</b> Router(config)# pseudowire-class mpls	Specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.
Step 4	<b>encapsulation mpls</b>  <b>Example:</b> Router(config-pw-class)# encapsulation mpls	Specifies MPLS encapsulation.
Step 5	<b>interface serial</b> <i>slot/subslot/port</i>  <b>Example:</b> Router(config)# interface serial0/0	Enters configuration mode for the serial interface. <b>Note</b> The slot number is always 0.
Step 6	Router(config)# <b>backup delay</b> <i>enable-delay</i> { <i>disable-delay</i>   <b>never</b> }	Configures the backup delay parameters. Where: <ul style="list-style-type: none"><li><i>enable-delay</i>—Time before the backup PW takes over for the primary PW.</li><li><i>disable-delay</i>—Time before the restored primary PW takes over for the backup PW.</li><li><b>never</b>—Disables switching from the backup PW to the primary PW.</li></ul>
Step 7	Router(config-if)# <b>xconnect 1.1.1.2</b> <b>101 encapsulation mpls</b>	Binds the Ethernet port interface to an attachment circuit to create a pseudowire.
Step 8	Router(config)# <b>backup peer</b> <i>peer-router-ip-address vcid</i> [ <b>pw-class</b> <i>pw-class name</i> ]	Defines the address and VC of the backup peer.
Step 9	<b>exit</b>  <b>Example:</b> Router(config)# <b>exit</b> Router#	Exits configuration mode.

## Verifying the Interface Configuration

You can use the following commands to verify your pseudowire configuration:

- **show cem circuit**—Displays information about the circuit state, administrative state, the CEM ID of the circuit, and the interface on which it is configured. If **xconnect** is configured under the circuit, the command output also includes information about the attached circuit.

```
Router# show cem circuit ?
<0-504>  CEM ID
detail  Detailed information of cem ckt(s)
interface CEM Interface
summary Display summary of CEM ckts
|       Output modifiers
```

```
Router# show cem circuit
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    --/--
```

- **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 Pkts: 25929           Dropped: 0
Egress Pkts: 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 summary**—Displays the number of circuits which are up or down per interface basis.

```
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.

# Sample Configurations

The following sections contain sample pseudowire configurations.

- [ATM over MPLS, page 12-22](#)
- [Ethernet over MPLS, page 12-30](#)

## ATM over MPLS

The following sections contain sample ATM over MPLS configurations:

- [Cell Packing Sample Configurations, page 12-22](#)
- [Cell Relay Sample Configurations, page 12-26](#)

## Cell Packing Sample Configurations

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

- [VC Mode, page 12-22](#)
- [VP Mode, page 12-24](#)

### VC Mode

#### CE 1 Configuration

```
interface Gig4/3/0
no negotiation auto
load-interval 30

interface Gig4/3/0
ip address 20.1.1.1 255.255.255.0
interface ATM4/2/4
no shut
exit
!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2
```

#### CE 2 Configuration

```
interface Gig8/8
no negotiation auto
load-interval 30

interface Gig8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
no shut
```

```
!  
interface ATM6/2/1.10 point  
ip address 50.1.1.2 255.255.255.0  
pvc 20/101  
encapsulation aal5snap  
  
!  
ip route 20.1.1.2 255.255.255.255 50.1.1.1
```

### PE 1 Configuration

```
interface Loopback0  
ip address 192.168.37.3 255.255.255.255  
  
!  
interface ATM0/0/0  
no shut  
  
!  
interface ATM0/0/0  
atm mcpt-timers 150 1000 4095  
  
interface ATM0/0/0.10 point  
pvc 20/101 l2transport  
encapsulation aal0  
cell-packing 20 mcpt-timer 1  
xconnect 192.168.37.2 100 encapsulation mpls  
  
!  
interface Gig0/3/0  
no shut  
ip address 40.1.1.1 255.255.0.0  
mpls ip  
  
!  
mpls ip  
mpls label protocol ldp  
mpls ldp router-id Loopback0 force  
mpls ldp graceful-restart  
  
router ospf 1  
network 40.1.0.0 0.0.255.255 area 1  
network 192.168.37.0 0.0.0.255 area 1  
nsf
```

### PE 2 Configuration

```
interface Loopback0  
ip address 192.168.37.2 255.255.255.255  
!  
interface ATM9/3/1  
no shut  
  
!  
interface ATM9/3/1  
atm mcpt-timers 150 1000 4095  
  
interface ATM9/3/1.10 point  
pvc 20/101 l2transport
```

```

encapsulation aal0
cell-packing 20 mcpt-timer 1
xconnect 192.168.37.3 100 encapsulation mpls

!
interface Gig6/2
no shut
ip address 40.1.1.2 255.255.0.0
mpls ip

!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart

router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

```

## VP Mode

### CE 1 Configuration

```

interface Gig4/3/0
no negotiation auto
load-interval 30

interface Gig4/3/0
ip address 20.1.1.1 255.255.255.0
interface ATM4/2/4

!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2

```

### CE 2 Configuration

```

!
interface Gig8/8
no negotiation auto
load-interval 30

interface Gig8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
no shut

```

```
!  
interface ATM6/2/1.10 point  
ip address 50.1.1.2 255.255.255.0  
pvc 20/101  
encapsulation aal5snap  
  
!  
ip route 20.1.1.2 255.255.255.255 50.1.1.1
```

### PE 1 Configuration

```
interface Loopback0  
ip address 192.168.37.3 255.255.255.255  
  
!  
interface ATM0/0/0  
no shut  
  
!  
interface ATM0/0/0  
atm mcpt-timers 150 1000 4095  
  
interface ATM0/0/0.50 multipoint  
atm pvp 20 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 Sample Configurations

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

- [VC Mode, page 12-26](#)
- [VP Mode, page 12-28](#)

### VC Mode

#### CE 1 Configuration

```

!
interface gigabitethernet4/3/0
no negotiation auto
load-interval 30

interface gigabitethernet4/3/0
ip address 20.1.1.1 255.255.255.0
!
interface ATM4/2/4
!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2
!

```

#### CE 2 Configuration

```

interface gigabitethernet8/8
no negotiation auto

```



```
load-interval 30

interface gigabitethernet8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
!
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 20.1.1.2 255.255.255.255 50.1.1.1
```

### PE 1 Configuration

```
!
interface Loopback0
ip address 192.168.37.3 255.255.255.255
!
interface ATM0/0/0
!

interface ATM0/0/0.10 point
pvc 20/101 l2transport
encapsulation aal0
xconnect 192.168.37.2 100 encapsulation mpls
!
interface gigabitethernet0/3/0
ip address 40.1.1.1 255.255.0.0
mpls ip

!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart

router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf
```

### PE 2 Configuration

```
!
interface Loopback0
ip address 192.168.37.2 255.255.255.255
!
interface ATM9/3/1
!
interface ATM9/3/1.10 point
pvc 20/101 l2transport
encapsulation aal0
xconnect 192.168.37.3 100 encapsulation mpls

!
interface gigabitethernet6/2
ip address 40.1.1.2 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
```

```

mpls ldp router-id Loopback0 force
mpls ldp graceful-restart

router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

```

## VP Mode

### CE 1 Configuration

```

!
interface gigabitethernet4/3/0
no negotiation auto
load-interval 30

interface gigabitethernet4/3/0
ip address 20.1.1.1 255.255.255.0
!
interface ATM4/2/4
!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2

```

### CE 2 Configuration

```

!
interface gigabitethernet8/8
no negotiation auto
load-interval 30

interface gigabitethernet8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
!
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 20.1.1.2 255.255.255.255 50.1.1.1

```

### PE 1 Configuration

```

interface Loopback0
ip address 192.168.37.3 255.255.255.255
!
!
interface ATM0/0/0

interface ATM0/0/0.50 multipoint
atm pvp 20 l2transport
xconnect 192.168.37.2 100 encapsulation mpls
!
interface gigabitethernet0/3/0

```

```
ip address 40.1.1.1 255.255.0.0
mpls ip

!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart

router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf
```

### PE 2 Configuration

```
interface Loopback0
ip address 192.168.37.2 255.255.255.255
!
!
interface ATM9/3/1

interface ATM9/3/1.50 multipoint
atm pvp 20 l2transport
xconnect 192.168.37.3 100 encapsulation mpls
!
interface gigabitethernet6/2
ip address 40.1.1.2 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart

router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf
```

## Ethernet over MPLS

### PE 1 Configuration

```

!
mpls label range 16 12000 static 12001 16000
mpls label protocol ldp
mpls ldp neighbor 10.1.1.1 targeted ldp
mpls ldp graceful-restart
multilink bundle-name authenticated
!
!
!
!
redundancy
mode sso
!
!
!
ip tftp source-interface GigabitEthernet0
!
!
interface Loopback0
ip address 10.5.5.5 255.255.255.255

!
interface GigabitEthernet0/0/4
no ip address
negotiation auto
!
service instance 2 ethernet
encapsulation dot1q 2
xconnect 10.1.1.1 1001 encapsulation mpls
!
service instance 3 ethernet
encapsulation dot1q 3
xconnect 10.1.1.1 1002 encapsulation mpls
!
!
interface GigabitEthernet0/0/5
ip address 172.7.7.77 255.0.0.0
negotiation auto
mpls ip
mpls label protocol ldp
!
router ospf 1
router-id 5.5.5.5
network 5.5.5.5 0.0.0.0 area 0
network 172.0.0.0 0.255.255.255 area 0
network 10.33.33.33 0.0.0.0 area 0
network 192.0.0.0 0.255.255.255 area 0
!

```

### PE 2 Configuration

```

!
mpls label range 16 12000 static 12001 16000
mpls label protocol ldp
mpls ldp neighbor 10.5.5.5 targeted ldp
mpls ldp graceful-restart
multilink bundle-name authenticated
!

```

```
!
redundancy
 mode sso
!
!
!
ip tftp source-interface GigabitEthernet0
!
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255

!
interface GigabitEthernet0/0/4
 no ip address
 negotiation auto
!
 service instance 2 ethernet
  encapsulation dot1q 2
  xconnect 10.5.5.5 1001 encapsulation mpls
!
 service instance 3 ethernet
  encapsulation dot1q 3
  xconnect 10.5.5.5 1002 encapsulation mpls
!
!
interface GigabitEthernet0/0/5
 ip address 172.7.7.7 255.0.0.0
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 10.1.1.1
 network 10.1.1.1 0.0.0.0 area 0
 network 172.0.0.0 0.255.255.255 area 0
 network 10.33.33.33 0.0.0.0 area 0
 network 192.0.0.0 0.255.255.255 area 0
!
```





## Configuring Quality of Service

---

The following sections describe support for Quality of Service features on the Cisco ASR 903 Series Router.

- [Understanding Quality of Service, page 13-1](#)
- [Configuring Quality of Service, page 13-1](#)

### 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 Frame Relay, 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 the [Quality of Service Solutions Configuration Guide Library, Cisco IOS XE Release 3S](#).

### 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 the [Quality of Service Solutions Configuration Guide Library, Cisco IOS XE Release 3S](#).

The following sections describe how to configure QoS on the Cisco ASR 903 Series Router:

- [Global QoS Limitations, page 13-2](#)
- [Classification, page 13-3](#)
- [Marking, page 13-5](#)
- [Policing, page 13-7](#)
- [Queuing, page 13-8](#)

- [Scheduling, page 13-8](#)

## Global QoS Limitations

The following limitations apply to multiple QoS features for the Cisco ASR 903 Series Router:

- QoS policies are not supported on LAG bundle interfaces or port channel interfaces.
- QoS policies are not supported on port-channel member links with Ethernet Flow Points (EFPs).
- QoS policies are not supported on physical interfaces configured with an Ethernet Flow Point (EFP) except for Trunk EFP interfaces, which do support QoS policies.
- 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 policy-map and class-map definitions while applied to an interface or Ethernet Flow Point is not supported.
- The ASR 903 router does not support a shared child QoS policy applied to a VLAN. As a workaround, you can create an individual child policy for each VLAN class.
- 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.
- QoS is not supported on TDM interfaces.
- The class-based QoS MIB is not supported.

## 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.
- Inner or outer VLAN classification must have a child policy that classifies based on cos (inner or outer), IP TOS byte, MPLS EXP, discard-class or qos-group.

## Sample Hierarchical Policy Designs

The following are examples of supported policy-map configurations:

- Three-Level Policy
  - Topmost policy: class-default
  - Middle policy: match vlan
  - Lowest policy: match ip precedence
- Two-Level Policy
  - Topmost policy: match vlan



- Lowest policy: match qos-group
- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match vlan
- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match mpls experimental topmost
- Flat policy: match ip dscp
- Flat policy: match vlan inner
- Flat policy: class-default

## Classification

The following sections describe classification features on the Cisco ASR 903 Series Router:

- [Classification Overview, page 13-3](#)
- [Ingress Classification Limitations, page 13-4](#)
- [Egress Classification Limitations, page 13-4](#)
- [Classifying Traffic using an Access Control List, page 13-4](#)

## Classification Overview

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.

The Cisco ASR 903 Series Router supports the following parameters with the **match** command in a QoS class-map.

- match cos (match up to 4 values)
- match cos inner
- match discard-class
- match ip dscp
- match ip precedence
- match mpls experimental topmost
- match qos-group
- match vlan
- match vlan inner

## 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 using an Access Control List

You can classify inbound packet based on an IP standard or IP extended access control list (ACL). Complete 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.
- The **neq** keyword is not supported with the access-list permit and ip access-list extended commands.
- This release does not support matching on multiple port numbers in a single ACE, as in the following command: **permit tcp any eq 23 45 80 any**
- 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
- By default, the Cisco ASR 903 Series Router uses port matching resources for security ACLs; the default settings do not provide the memory required for port matching through QoS ACLs. To make resources available for QoS ACLs, set the `ROMMON_QOS_ACL_PORTRANGE_OVERRIDE` to 2; this setting configures the router to use the Ternary content-addressable memory (TCAM) expansion method memory for security ACL operations. Setting the `ROMMON_QOS_ACL_PORTRANGE_OVERRIDE` value to 1 allows security ACLs to use the same memory resources as QoS ACLs, which can disable or limit QoS ACL 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.
- **show romvar**- Displays current rommon variable settings, including `ROMMON_QOS_ACL_PORTRANGE_OVERRIDE`.

For more information about configuring QoS, see the [Quality of Service Solutions Configuration Guide Library, Cisco IOS XE Release 3S](#). For more information about configuring access control lists, see the [Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S](#).

## Marking

The following sections describe marking features on the Cisco ASR 903 Series Router:

- [Marking Limitations, page 13-6](#)
- [Ingress Marking Limitations, page 13-6](#)
- [Egress Marking Limitations, page 13-6](#)

## Marking Limitations

The only supports the following parameters with the **set** command:

- set cos
- set cos inner (ingress marking)
- set discard-class
- set ip dscp
- set ip precedence
- set mpls experimental topmost
- set mpls experimental imposition (ingress marking)
- 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.
- set cos inner—This command modifies the outermost 802.1q header of a packet. This set action will modify the outermost 802.1q header of the packet after any ingress rewrite operations. This action modifies the packet even if there is no push action on egress. Any push operation on egress will use the value applied by "set cos" or by default the COS value of the outermost 802.1q header when the packet arrived at the ingress interface.

### 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 3.5.2 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 eperimental topmost** command is supported for marking MPLS Exp bits; other commands for marking MPLS Exp bits are not supported.

# Policing

The following sections describe policing features on the Cisco ASR 903 Series Router:

- [Policing Overview, page 13-7](#)
- [Ingress Policing Limitations, page 13-8](#)
- [Egress Policing Limitations, page 13-8](#)

## Policing Overview

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)

## Supported Commands

The Cisco ASR 903 Series Router supports the following policing commands on ingress interfaces:

- **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 cir** [**bc conform-burst**] [**pir pir**] [**be peak-burst**] [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]]]

## 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

## Hierarchical Policing

Hierarchical Policing is not supported.

## 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

The Cisco ASR 903 Series Router does not support policing on egress interfaces.

## Queuing

The following sections describe queuing features on the Cisco ASR 903 Series Router:

- [Queuing Overview, page 13-8](#)
- [Ingress Queuing Limitations, page 13-8](#)
- [Egress Queuing Limitations, page 13-8](#)

## Queuing Overview

The Cisco ASR 903 Series Router supports tail drop queuing for congestion management, which allows you to control congestion by determining the order in which packets are sent based on assigned priority.

## 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.

## Scheduling

The following sections describe scheduling features on the Cisco ASR 903 Series Router:

- [Scheduling Overview, page 13-9](#)
- [Ingress Scheduling Limitations, page 13-9](#)
- [Egress Scheduling Limitations, page 13-9](#)

## Scheduling Overview

The Cisco ASR 903 Series Router supports scheduling on egress interfaces. Scheduling is not supported on ingress interfaces.

## 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 can not 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.







# 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 903 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 903 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 903 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 903 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 14-1 Tracing Levels and Descriptions**

Trace Level	Level Number	Description
Emergency	0	The message is regarding an issue that makes the system unusable.
Alert	1	The message is regarding an action that must be taken immediately.
Critical	2	The message is regarding a critical condition. This is the default setting.
Error	3	The message is regarding a system error.
Warning	4	The message is regarding a system warning
Notice	5	The message is regarding a significant issue, but the router is still working normally.
Informational	6	The message is useful for informational purposes only.
Debug	7	The message provides debug-level output.
Verbose	8	All possible tracing messages are sent.
Noise	-	All possible trace messages for the module are logged.  The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.

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

The default tracing level for every module on the Cisco ASR 903 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 903 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 903 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
evutil                                     Notice
file_alloc                                 Notice
fman_rp                                    Notice
fpm                                         Notice
fw                                          Notice
icmp                                       Notice
interfaces                                 Notice
iosd                                       Notice
ipc                                         Notice
ipclog                                    Notice
iphc                                       Notice
ipsec                                      Notice
mgmte-acl                                  Notice
```

mlp	Notice
mqipc	Notice
nat	Notice
nbar	Notice
netflow	Notice
om	Notice
peer	Notice
qos	Notice
route-map	Notice
sbc	Notice
services	Notice
sw_wdog	Notice
tcl_acl_config_type	Notice
tcl_acl_db_type	Notice
tcl_cdlcore_message	Notice
tcl_cef_config_common_type	Notice
tcl_cef_config_type	Notice
tcl_dpibdb_config_type	Notice
tcl_fman_rp_comm_type	Notice
tcl_fman_rp_message	Notice
tcl_fw_config_type	Notice
tcl_hapi_tcl_type	Notice
tcl_icmp_type	Notice
tcl_ip_options_type	Notice
tcl_ipc_ack_type	Notice
tcl_ipsec_db_type	Notice
tcl_mcp_comm_type	Notice
tcl_mlp_config_type	Notice
tcl_mlp_db_type	Notice
tcl_om_type	Notice
tcl_ui_message	Notice
tcl_ui_type	Notice
tcl_urpf_config_type	Notice
tdllib	Notice
trans_avl	Notice
uihandler	Notice
uipeer	Notice
uistatus	Notice
urpf	Notice
vista	Notice
wccp	Notice

## Setting a Tracing Level

To set a tracing level for any module on the Cisco ASR 903 Series Router, or for all modules within a process on the Cisco ASR 903 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 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in
slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in
slot 0
```





---

## Symbols

<cr> 1-9

? command 1-9

---

## 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

cautions, usage in text i-xiv

CEF 11-1

CEF for PFC2

    See CEF

circuit emulation service over packet-switched network 11-2

Cisco IOS configuration changes, saving 1-12

command-line interface, getting help 1-9

command line processing 1-7

command modes, understanding 1-2

commands

    context-sensitive help for abbreviating 1-9

    default form, using 1-12

    no form, using 1-12

command syntax

    conventions i-xiii

    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

console, accessing 1-4

console, accessing using a direct connection 1-4

console, accessing using telnet 1-6

console, configuring a transport map 2-3

console, connecting 1-4

console, traffic handling 2-2

console, using 1-5

console, viewing handling configuration 2-12

copy command 7-7

crashinfo files, overview 5-4

---

## D

diagnostic configuration mode, summary of 1-3

diagnostic mode, overview 1-3

dot1q encapsulation 7-6

    configuration (example) 7-17

---

## E

e1 bert pattern command 8-8

## encapsulation

- dot1q [7-6](#)
  - configuration (example) [7-17](#)
- SNAP [7-5](#)

**F**

- field programmable hardware device upgrade [5-3](#)
- file systems, overview [5-3](#)
- filtering output, show and more commands [1-14](#)
  - for [7-11](#)
- framing, configuring [8-5](#)

**G**

## Gigabit Ethernet Interface Modules

- configuring [7-1](#)
- modifying MTU [7-5](#)

global configuration mode, summary of [1-2](#)

**H**

- hardware, upgrading in the field [5-3](#)
- 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](#)

**I**

- IEEE 802.1Q encapsulation [7-6](#)
  - configuration (example) [7-17](#)
- interface
  - basic configuration (example) [7-16](#)
  - 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](#)

**K**

- keyboard shortcuts [1-7](#)

**L**

- lost+found directory, overview [5-4](#)

**M**

- Management Ethernet Interface, common tasks [3-3](#)
- Management Ethernet interface, interface numbering [3-2](#)
- 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) [7-16](#)
  - default size [7-5](#)
  - interface MTU
    - additional overhead [7-5](#)
    - configuration guidelines [7-5](#)
    - configuring [7-5](#)
    - description [7-5](#)
    - verifying [7-6](#)
  - 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, 7-5](#)

---

## N

negotiation auto command [7-7](#)  
 no negotiation auto command [7-7](#)  
 no shut command [7-3](#)  
 notes, usage in text [i-xiv](#)  
 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  
 rommon image, overview [5-3](#)  
 ROM monitor mode, summary of [1-3](#)  
 RPAccess, Overview [5-2](#)

RPBBase, Overview [5-2](#)  
 RPControl, Overview [5-2](#)  
 RPIOS, Overview [5-2](#)  
 running configuration, saving to NVRAM [7-7](#)

---

## S

Secure Shell (SSH), configuring persistent SSH [2-9](#)  
 Secure Shell (SSH), persistent [2-2](#)  
 Secure Shell (SSH), persistent SSH restrictions [2-17](#)  
 Secure Shell (SSH), viewing handling configuration [2-12](#)  
 show history command [1-8](#)  
 show hw-module subslot transceiver idprom  
 command [7-10](#)  
 show interface serial command [8-10](#)  
 show interfaces gigabitethernet command [7-6](#)  
 show standby command [7-4](#)  
 shutdown command [7-8](#)  
 SNAP (Subnetwork Access Protocol) encapsulation [7-5](#)  
 Software Packaging, Overview [5-1](#)  
 Stateful Switchover (SSO), overview [4-2](#)  
 Stateful Switchover, Supported Protocols and  
 Applications [4-2](#)  
 Step1 [8-16](#)  
 Step4 [8-16](#)  
 Structure-agnostic TDM over Packet [11-1](#)  
 Structure-agnostic TDM over Packet (SaToP) [11-1](#)

---

## T

T1/E1 Interface Module [8-1](#)  
     configuring [8-2](#)  
     framing [8-5](#)  
     verifying the configuration [8-17](#)  
 Tab key, command completion [1-9](#)  
 telnet, configuring persistent telnet [2-5](#)  
 telnet, persistent [2-2](#)  
 telnet, persistent telnet restrictions [2-17](#)  
 telnet, using [1-5](#)

telnet, using to access console [1-6](#)  
telnet, viewing handling configuration [2-12](#)  
Tracing, how tracing works [13-1](#)  
Tracing, overview [13-1](#)  
Tracing, setting a tracing level [13-4](#)  
Tracing, tracing levels [13-2](#)  
Tracing, viewing a tracing level [13-3](#)  
Tracing, viewing trace logs [13-5](#)

---

## U

upgrading field programmable hardware device [5-3](#)  
user EXEC mode, summary of [1-2](#)

---

## V

VLANs (virtual LANs)  
    configuration (example) [7-17](#)